Nessus Report

Report

24/Feb/2012:18:30:37 GMT

Table Of Contents

Vulnerabilities By Host

192.168.150.131

Scan Information

Start time:	Fri Feb 24 18:29:52 2012
End time:	Fri Feb 24 18:30:37 2012

Host Information

DNS Name:	SECURITYFAIL
IP:	192.168.150.131
MAC Address:	00:0c:29:16:e8:6c
OS:	Linux Kernel 2.6.31-23-generic-pae on Ubuntu 9.10

Results Summary

Critical	High	Medium	Low	Info	Total
2	21	31	3	63	120

Results Details

0/tcp

50044 - USN-1000-1 : linux, linux-ec2, linux-source-2.6.15 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Joel Becker discovered that OCFS2 did not correctly validate on-disk symlink structures. If an attacker were able to trick a user or automated system into mounting a specially crafted filesystem, it could crash the system or exposde kernel memory, leading to a loss of privacy. (Ubuntu 6.06 LTS, 8.04 LTS, and 9.04 were not affected.)
Al Viro discovered a race condition in the TTY driver. A local attacker could exploit this to crash the system, leading to a denial of service. (Only Ubuntu 9.04 and 9.10 were affected.) (CVE-2009-4895)
Dan Rosenberg discovered that the MOVE_EXT ext4 ioctl did not correctly check file permissions. A local attacker could overwrite append-only files, leading to potential data loss. (Only Ubuntu 9.10 was affected.) (CVE-2010-2066)
Dan Rosenberg discovered that the swapexit xfs ioctl did not correctly check file permissions. A local attacker could exploit this to read from write-only files, leading to a loss of privacy. (Only Ubuntu 8.04 LTS, 9.04, and 9.10 were affected.) (CVE-2010-2226)
Suresh Jayaraman discovered that CIFS did not correctly validate certain response packats. A remote attacker could send specially crafted traffic that would crash the system, leading to a denial of service. (Ubuntu 10.04 LTS and 10.10 were not affected.) (CVE-2010-2248)
Ben Hutchings discovered that the ethtool interface did not correctly check certain sizes. A local attacker could perform malicious ioctl calls that could crash the system, leading to a denial of service.
(Only Ubuntu 9.10 and 10.04 LTS were affected.) (CVE-2010-2478, CVE-2010-3084)
James Chapman discovered that L2TP did not correctly evaluate checksum capabilities. If an attacker could make malicious routing changes, they could crash the system, leading to a denial of service.
(Only Ubuntu 9.10 was affected.) (CVE-2010-2495)
Neil Brown discovered that NFSv4 did not correctly check certain write requests. A remote attacker could send specially crafted traffic that could crash the system or possibly gain root privileges.
(Ubuntu 10.04 LTS and 10.10 were not affected.) (CVE-2010-2521)
David Howells discovered that DNS resolution in CIFS could be spoofed. A local attacker could exploit this to control DNS replies, leading to a loss of privacy and possible privilege escalation. (Only Ubuntu 9.10 was affected.) (CVE-2010-2524)
Bob Peterson discovered that GFS2 rename operations did not correctly validate certain sizes. A local attacker could exploit this to crash the system, leading to a denial of service. (Only Ubuntu 8.04 LTS, 9.04, and 9.10 were affected.) (CVE-2010-2798)
Eric Dumazet discovered that many network functions could leak kernel stack contents. A local attacker could exploit this to read portions of kernel memory, leading to a loss of privacy. (Ubuntu 10.10 was not affected.) (CVE-2010-2942, CVE-2010-3477)
Sergey Vlasov discovered that JFS did not correctly handle certain extended attributes. A local attacker could bypass namespace access rules, leading to a loss of privacy. (Ubuntu 10.04 LTS and 10.10 were not affected.) (CVE-2010-2946)

Tavis Ormandy discovered that the IRDA subsystem did not correctly shut down. A local attacker could exploit this to cause the system to crash or possibly gain root privileges. (Ubuntu 6.06 LTS and 10.10 were not affected.) (CVE-2010-2954)
Brad Spengler discovered that the wireless extensions did not correctly validate certain request sizes. A local attacker could exploit this to read portions of kernel memory, leading to a loss of privacy. (Only Ubuntu 9.04, 9.10 and 10.04 LTS were affected.) (CVE-2010-2955)
Tavis Ormandy discovered that the session keyring did not correctly check for its parent. On systems without a default session keyring, a local attacker could exploit this to crash the system, leading to a denial of service. (Only Ubuntu 10.04 LTS was affected.) (CVE-2010-2960)
Kees Cook discovered that the V4L1 32bit compat interface did not correctly validate certain parameters. A local attacker on a 64bit system with access to a video device could exploit this to gain root privileges. (Ubuntu 6.06 LTS was not affected.) (CVE-2010-2963)
Toshiyuki Okajima discovered that ext4 did not correctly check certain parameters. A local attacker could exploit this to crash the system or overwrite the last block of large files. (Only Ubuntu 8.04 LTS, 9.04, and 9.10 were affected.) (CVE-2010-3015)
Tavis Ormandy discovered that the AIO subsystem did not correctly validate certain parameters. A local attacker could exploit this to crash the system or possibly gain root privileges. (Ubuntu 10.10 was not affected.) (CVE-2010-3067)
Dan Rosenberg discovered that certain XFS ioctls leaked kernel stack contents. A local attacker could exploit this to read portions of kernel memory, leading to a loss of privacy. (Ubuntu 6.06 LTS and 10.10 were not affected.) (CVE-2010-3078)
Tavis Ormandy discovered that the OSS sequencer device did not correctly shut down. A local attacker could exploit this to crash the system or possibly gain root privileges. (Ubuntu 10.10 was not affected.) (CVE-2010-3080)
Dan Rosenberg discovered that the ROSE driver did not correctly check parameters. A local attacker with access to a ROSE network device could exploit this to crash the system or possibly gain root privileges. (Ubuntu 10.10 was not affected.) (CVE-2010-3310)
Thomas Dreibholz discovered that SCTP did not correctly handle appending packet chunks. A remote attacker could send specially crafted traffic to crash the system, leading to a denial of service.
(Ubuntu 10.10 was not affected.) (CVE-2010-3432)
Dan Rosenberg discovered that the CD driver did not correctly check parameters. A local attacker could exploit this to read arbitrary kernel memory, leading to a loss of privacy. (CVE-2010-3437)
Dan Rosenberg discovered that the Sound subsystem did not correctly validate parameters. A local attacker could exploit this to crash the system, leading to a denial of service. (Ubuntu 10.10 was not affected.) (CVE-2010-3442)
Dan Rosenberg discovered that SCTP did not correctly handle HMAC calculations. A remote attacker could send specially crafted traffic that would crash the system, leading to a denial of service. (Ubuntu 6.06 LTS was not affected.) (CVE-2010-3705)
Dan Rosenberg discovered that the RDS network protocol did not correctly check certain parameters. A local attacker could exploit this gain root privileges. (Only Ubuntu 9.10, 10.04 LTS, and 10.10 were affected.) (CVE-2010-3904)

See Also

http://www.ubuntu.com/usn/usn-1000-1/

Solution

Update the affected package(s).

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

CVE	CVE-2009-4895
CVE	CVE-2010-2066
CVE	CVE-2010-2226
CVE	CVE-2010-2248
CVE	CVE-2010-2478
CVE	CVE-2010-2495
CVE	CVE-2010-2521

CVE	CVE-2010-2524
CVE	CVE-2010-2798
CVE	CVE-2010-2942
CVE	CVE-2010-2946
CVE	CVE-2010-2954
CVE	CVE-2010-2955
CVE	CVE-2010-2960
CVE	CVE-2010-2963
CVE	CVE-2010-3015
CVE	CVE-2010-3067
CVE	CVE-2010-3078
CVE	CVE-2010-3080
CVE	CVE-2010-3084
CVE	CVE-2010-3310
CVE	CVE-2010-3432
CVE	CVE-2010-3437
CVE	CVE-2010-3442
CVE	CVE-2010-3477
CVE	CVE-2010-3705
CVE	CVE-2010-3904
XREF	USN:1000-1

Exploitable with

CANVAS (true)

Ports

tcp/0

```
  - Installed package : linux-libc-dev_2.6.31-21.59
    Fixed package     : linux-libc-dev_2.6.31-22.67
```

49805 - USN-1003-1 : openssl vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that OpenSSL incorrectly handled return codes from the bn_wexpand function calls. A remote attacker could trigger this flaw in services that used SSL to cause a denial of service or possibly execute arbitrary code with application privileges. This issue only affected Ubuntu 6.06 LTS, 8.04 LTS, 9.04 and 9.10. (CVE-2009-3245)
It was discovered that OpenSSL incorrectly handled certain private keys with an invalid prime. A remote attacker could trigger this flaw in services that used SSL to cause a denial of service or possibly execute arbitrary code with

application privileges. The default compiler options for affected releases should reduce the vulnerability to a denial of service. (CVE-2010-2939)

See Also

http://www.ubuntu.com/usn/usn-1003-1/

Solution

Update the affected package(s).

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

CVE	CVE-2009-3245
CVE	CVE-2010-2939
XREF	OSVDB:62844
XREF	OSVDB:66946
XREF	IAVA:2010-A-0042
XREF	USN:1003-1
XREF	CWE:20

Ports

tcp/0

```
  - Installed package : libssl0.9.8_0.9.8g-16ubuntu3.1
    Fixed package     : libssl0.9.8_0.9.8g-16ubuntu3.3

  - Installed package : openssl_0.9.8g-16ubuntu3.1
    Fixed package     : openssl_0.9.8g-16ubuntu3.3
```

48261 - USN-968-1 : base-files vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that the Ubuntu image shipped on some Dell Latitude 2110 systems was accidentally configured to allow unauthenticated package installations. A remote attacker intercepting network communications or a malicious archive mirror server could exploit this to trick the user into installing unsigned packages, resulting in arbitrary code execution with root privileges.

See Also

http://www.ubuntu.com/usn/usn-968-1/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

CVE	CVE-2010-0834

XREF	OSVDB:66963
XREF	USN:968-1

Ports

tcp/0

```
  - Installed package : base-files_5.0.0ubuntu7
    Fixed package     : base-files_5.0.0ubuntu7.1
```

46810 - USN-947-1 : linux, linux-source-2.6.15 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that the Linux kernel did not correctly handle memory protection of the Virtual Dynamic Shared Object page when running a 32-bit application on a 64-bit kernel. A local attacker could exploit this to cause a denial of service. (Only affected Ubuntu 6.06 LTS.) (CVE-2009-4271)
It was discovered that the r8169 network driver did not correctly check the size of Ethernet frames. A remote attacker could send specially crafted traffic to crash the system, leading to a denial of service. (CVE-2009-4537)
Wei Yongjun discovered that SCTP did not correctly validate certain chunks. A remote attacker could send specially crafted traffic to monopolize CPU resources, leading to a denial of service. (Only affected Ubuntu 6.06 LTS.) (CVE-2010-0008)
It was discovered that KVM did not correctly limit certain privileged IO accesses on x86. Processes in the guest OS with access to IO regions could gain further privileges within the guest OS. (Did not affect Ubuntu 6.06 LTS.) (CVE-2010-0298, CVE-2010-0306, CVE-2010-0419)
Evgeniy Polyakov discovered that IPv6 did not correctly handle certain TUN packets. A remote attacker could exploit this to crash the system, leading to a denial of service. (Only affected Ubuntu 8.04 LTS.) (CVE-2010-0437)
Sachin Prabhu discovered that GFS2 did not correctly handle certain locks. A local attacker with write access to a GFS2 filesystem could exploit this to crash the system, leading to a denial of service.
(CVE-2010-0727)
Jamie Strandboge discovered that network virtio in KVM did not correctly handle certain high-traffic conditions. A remote attacker could exploit this by sending specially crafted traffic to a guest OS, causing the guest to crash, leading to a denial of service. (Only affected Ubuntu 8.04 LTS.) (CVE-2010-0741)
Marcus Meissner discovered that the USB subsystem did not correctly handle certain error conditions. A local attacker with access to a USB device could exploit this to read recently used kernel memory, leading to a loss of privacy and potentially root privilege escalation. (CVE-2010-1083)
Neil Brown discovered that the Bluetooth subsystem did not correctly handle large amounts of traffic. A physically proximate remote attacker could exploit this by sending specially crafted traffic that would consume all available system memory, leading to a denial of service. (Ubuntu 6.06 LTS and 10.04 LTS were not affected.) (CVE-2010-1084)
Jody Bruchon discovered that the sound driver for the AMD780V did not correctly handle certain conditions. A local attacker with access to this hardward could exploit the flaw to cause a system crash, leading to a denial of service.
(CVE-2010-1085)
Ang Way Chuang discovered that the DVB driver did not correctly handle certain MPEG2-TS frames. An attacker could exploit this by delivering specially crafted frames to monopolize CPU resources, leading to a denial of service. (Ubuntu 10.04 LTS was not affected.) (CVE-2010-1086)
Trond Myklebust discovered that NFS did not correctly handle truncation under certain conditions. A local attacker with write access to an NFS share could exploit this to crash the system, leading to a denial of service. (Ubuntu 10.04 LTS was not affected.) (CVE-2010-1087)
Al Viro discovered that automount of NFS did not correctly handle symlinks under certain conditions. A local attacker could exploit this to crash the system, leading to a denial of service. (Ubuntu 6.06 LTS and Ubuntu 10.04 LTS were not affected.) (CVE-2010-1088)
Matt McCutchen discovered that ReiserFS did not correctly protect xattr files in the .reiserfs_priv directory. A local attacker could exploit this to gain root privileges or crash the system, leading to a denial of service. (CVE-2010-1146)
Eugene Teo discovered that CIFS did not correctly validate arguments when creating new files. A local attacker could exploit this to crash the system, leading to a denial of service, or possibly gain root privileges if mmap_min_addr was not set. (CVE-2010-1148)
Catalin Marinas and Tetsuo Handa discovered that the TTY layer did not correctly release process IDs. A local attacker could exploit this to consume kernel resources, leading to a denial of service.
(CVE-2010-1162)
Neil Horman discovered that TIPC did not correctly check its internal state. A local attacker could send specially crafted packets via AF_TIPC that would cause the system to crash, leading to a denial of service. (Ubuntu 6.06 LTS was not affected.) (CVE-2010-1187)

Masayuki Nakagawa discovered that IPv6 did not correctly handle certain settings when listening. If a socket were listening with the IPV6_RECVPKTINFO flag, a remote attacker could send specially crafted traffic that would cause the system to crash, leading to a denial of service. (Only Ubuntu 6.06 LTS was affected.) (CVE-2010-1188)
Oleg Nesterov discovered that the Out-Of-Memory handler did not correctly handle certain arrangements of processes. A local attacker could exploit this to crash the system, leading to a denial of service. (CVE-2010-1488)

See Also

http://www.ubuntu.com/usn/usn-947-1/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

References

CVE	CVE-2009-4271
CVE	CVE-2009-4537
CVE	CVE-2010-0008
CVE	CVE-2010-0298
CVE	CVE-2010-0306
CVE	CVE-2010-0419
CVE	CVE-2010-0437
CVE	CVE-2010-0727
CVE	CVE-2010-0741
CVE	CVE-2010-1083
CVE	CVE-2010-1084
CVE	CVE-2010-1085
CVE	CVE-2010-1086
CVE	CVE-2010-1087
CVE	CVE-2010-1088
CVE	CVE-2010-1146
CVE	CVE-2010-1148
CVE	CVE-2010-1162
CVE	CVE-2010-1187
CVE	CVE-2010-1188
CVE	CVE-2010-1488
XREF	IAVA:2010-A-0037
XREF	USN:947-1

XREF	CWE:264

Ports

tcp/0

```
  - Installed package : linux-libc-dev_2.6.31-21.59
    Fixed package     : linux-libc-dev_2.6.31-22.60
```

51453 - USN-1041-1 : linux, linux-ec2 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Dan Rosenberg discovered that the btrfs filesystem did not correctly validate permissions when using the clone function. A local attacker could overwrite the contents of file handles that were opened for append-only, or potentially read arbitrary contents, leading to a loss of privacy. Only Ubuntu 9.10 was affected. (CVE-2010-2537, CVE-2010-2538)
Dave Chinner discovered that the XFS filesystem did not correctly order inode lookups when exported by NFS. A remote attacker could exploit this to read or write disk blocks that had changed file assignement or had become unlinked, leading to a loss of privacy.
(CVE-2010-2943)
Kees Cook discovered that the Intel i915 graphics driver did not correctly validate memory regions. A local attacker with access to the video card could read and write arbitrary kernel memory to gain root privileges. Ubuntu 10.10 was not affected. (CVE-2010-2962)
Robert Swiecki discovered that ftrace did not correctly handle mutexes. A local attacker could exploit this to crash the kernel, leading to a denial of service. (CVE-2010-3079)
Dan Rosenberg discovered that several network ioctls did not clear kernel memory correctly. A local user could exploit this to read kernel stack memory, leading to a loss of privacy. (CVE-2010-3296, CVE-2010-3297, CVE-2010-3298)
Ben Hawkes discovered that the Linux kernel did not correctly filter registers on 64bit kernels when performing 32bit system calls. On a 64bit system, a local attacker could manipulate 32bit system calls to gain root privileges. The Ubuntu EC2 kernels needed additional fixing. (CVE-2010-3301)
Brad Spengler discovered that stack memory for new a process was not correctly calculated. A local attacker could exploit this to crash the system, leading to a denial of service. (CVE-2010-3858)
Kees Cook discovered that the ethtool interface did not correctly clear kernel memory. A local attacker could read kernel heap memory, leading to a loss of privacy. (CVE-2010-3861)
Kees Cook and Vasiliy Kulikov discovered that the shm interface did not clear kernel memory correctly. A local attacker could exploit this to read kernel stack memory, leading to a loss of privacy.
(CVE-2010-4072)

See Also

http://www.ubuntu.com/usn/usn-1041-1/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

7.9 (CVSS2#AV:N/AC:M/Au:S/C:C/I:C/A:N)

References

CVE	CVE-2010-2537
CVE	CVE-2010-2538
CVE	CVE-2010-2943
CVE	CVE-2010-2962
CVE	CVE-2010-3079
CVE	CVE-2010-3296

CVE	CVE-2010-3297
CVE	CVE-2010-3298
CVE	CVE-2010-3301
CVE	CVE-2010-3858
CVE	CVE-2010-3861
CVE	CVE-2010-4072
XREF	USN:1041-1

Ports

tcp/0

```
  - Installed package : linux-libc-dev_2.6.31-21.59
    Fixed package     : linux-libc-dev_2.6.31-22.70
```

49306 - USN-989-1 : php5 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Auke van Slooten discovered that PHP incorrectly handled certain xmlrpc requests. An attacker could exploit this issue to cause the PHP server to crash, resulting in a denial of service. This issue only affected Ubuntu 6.06 LTS, 8.04 LTS, 9.04 and 9.10.
(CVE-2010-0397)
It was discovered that the pseudorandom number generator in PHP did not provide the expected entropy. An attacker could exploit this issue to predict values that were intended to be random, such as session cookies. This issue only affected Ubuntu 6.06 LTS, 8.04 LTS, 9.04 and 9.10. (CVE-2010-1128)
It was discovered that PHP did not properly handle directory pathnames that lacked a trailing slash character. An attacker could exploit this issue to bypass safe_mode restrictions. This issue only affected Ubuntu 6.06 LTS, 8.04 LTS, 9.04 and 9.10. (CVE-2010-1129)
Grzegorz Stachowiak discovered that the PHP session extension did not properly handle semicolon characters. An attacker could exploit this issue to bypass safe_mode restrictions. This issue only affected Ubuntu 8.04 LTS, 9.04 and 9.10. (CVE-2010-1130)
Stefan Esser discovered that PHP incorrectly decoded remote HTTP chunked encoding streams. An attacker could exploit this issue to cause the PHP server to crash and possibly execute arbitrary code with application privileges. This issue only affected Ubuntu 10.04 LTS. (CVE-2010-1866)
Mateusz Kocielski discovered that certain PHP SQLite functions incorrectly handled empty SQL queries. An attacker could exploit this issue to possibly execute arbitrary code with application privileges.
(CVE-2010-1868)
Mateusz Kocielski discovered that PHP incorrectly handled certain arguments to the fnmatch function. An attacker could exploit this flaw and cause the PHP server to consume all available stack memory, resulting in a denial of service. (CVE-2010-1917)
Stefan Esser discovered that PHP incorrectly handled certain strings in the phar extension. An attacker could exploit this flaw to possibly view sensitive information. This issue only affected Ubuntu 10.04 LTS. (CVE-2010-2094, CVE-2010-2950)
Stefan Esser discovered that PHP incorrectly handled deserialization of SPLObjectStorage objects. A remote attacker could exploit this issue to view sensitive information and possibly execute arbitrary code with application privileges. This issue only affected Ubuntu 8.04 LTS, 9.04, 9.10 and 10.04 LTS. (CVE-2010-2225)
It was discovered that PHP incorrectly filtered error messages when limits for memory, execution time, or recursion were exceeded. A remote attacker could exploit this issue to possibly view sensitive information. (CVE-2010-2531)
Stefan Esser discovered that the PHP session serializer incorrectly handled the PS_UNDEF_MARKER marker. An attacker could exploit this issue to alter arbitrary session variables. (CVE-2010-3065)

See Also

http://www.ubuntu.com/usn/usn-989-1/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

CVE	CVE-2010-0397
CVE	CVE-2010-1128
CVE	CVE-2010-1129
CVE	CVE-2010-1130
CVE	CVE-2010-1866
CVE	CVE-2010-1868
CVE	CVE-2010-1917
CVE	CVE-2010-2094
CVE	CVE-2010-2225
CVE	CVE-2010-2531
CVE	CVE-2010-2950
CVE	CVE-2010-3065
XREF	OSVDB:62582
XREF	OSVDB:62583
XREF	OSVDB:63078
XREF	OSVDB:63323
XREF	OSVDB:64526
XREF	OSVDB:64527
XREF	OSVDB:64607
XREF	OSVDB:65755
XREF	OSVDB:66086
XREF	OSVDB:66798
XREF	OSVDB:66805
XREF	USN:989-1

Ports

tcp/0

```
  - Installed package : libapache2-mod-php5_5.2.10.dfsg.1-2ubuntu6.4
    Fixed package     : libapache2-mod-php5_5.2.10.dfsg.1-2ubuntu6.5

  - Installed package : php5_5.2.10.dfsg.1-2ubuntu6.4
    Fixed package     : php5_5.2.10.dfsg.1-2ubuntu6.5

  - Installed package : php5-common_5.2.10.dfsg.1-2ubuntu6.4
    Fixed package     : php5-common_5.2.10.dfsg.1-2ubuntu6.5
```

```
- Installed package : php5-mysql_5.2.10.dfsg.1-2ubuntu6.4
  Fixed package     : php5-mysql_5.2.10.dfsg.1-2ubuntu6.5
```

52476 - USN-1073-1 : linux, linux-ec2 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Gleb Napatov discovered that KVM did not correctly check certain privileged operations. A local attacker with access to a guest kernel could exploit this to crash the host system, leading to a denial of service. (CVE-2010-0435)
Dan Jacobson discovered that ThinkPad video output was not correctly access controlled. A local attacker could exploit this to hang the system, leading to a denial of service. (CVE-2010-3448)
It was discovered that KVM did not correctly initialize certain CPU registers. A local attacker could exploit this to crash the system, leading to a denial of service. (CVE-2010-3698)
Dan Rosenberg discovered that the Linux kernel TIPC implementation contained multiple integer signedness errors. A local attacker could exploit this to gain root privileges. (CVE-2010-3859)
Thomas Pollet discovered that the RDS network protocol did not check certain iovec buffers. A local attacker could exploit this to crash the system or possibly execute arbitrary code as the root user.
(CVE-2010-3865)
Dan Rosenberg discovered that the Linux kernel X.25 implementation incorrectly parsed facilities. A remote attacker could exploit this to crash the kernel, leading to a denial of service. (CVE-2010-3873)
Dan Rosenberg discovered that the CAN protocol on 64bit systems did not correctly calculate the size of certain buffers. A local attacker could exploit this to crash the system or possibly execute arbitrary code as the root user.
(CVE-2010-3874)
Vasiliy Kulikov discovered that the Linux kernel X.25 implementation did not correctly clear kernel memory. A local attacker could exploit this to read kernel stack memory, leading to a loss of privacy.
(CVE-2010-3875)
Vasiliy Kulikov discovered that the Linux kernel sockets implementation did not properly initialize certain structures. A local attacker could exploit this to read kernel stack memory, leading to a loss of privacy. (CVE-2010-3876)
Vasiliy Kulikov discovered that the TIPC interface did not correctly initialize certain structures. A local attacker could exploit this to read kernel stack memory, leading to a loss of privacy.
(CVE-2010-3877)
Nelson Elhage discovered that the Linux kernel IPv4 implementation did not properly audit certain bytecodes in netlink messages. A local attacker could exploit this to cause the kernel to hang, leading to a denial of service.
(CVE-2010-3880)
Dan Rosenberg discovered that the USB subsystem did not correctly initialize certian structures. A local attacker could exploit this to read kernel stack memory, leading to a loss of privacy.
(CVE-2010-4074)
Dan Rosenberg discovered that the SiS video driver did not correctly clear kernel memory. A local attacker could exploit this to read kernel stack memory, leading to a loss of privacy. (CVE-2010-4078)
Dan Rosenberg discovered that the ivtv V4L driver did not correctly initialize certian structures. A local attacker could exploit this to read kernel stack memory, leading to a loss of privacy.
(CVE-2010-4079)
Dan Rosenberg discovered that the RME Hammerfall DSP audio interface driver did not correctly clear kernel memory. A local attacker could exploit this to read kernel stack memory, leading to a loss of privacy. (CVE-2010-4080, CVE-2010-4081)
Dan Rosenberg discovered that the VIA video driver did not correctly clear kernel memory. A local attacker could exploit this to read kernel stack memory, leading to a loss of privacy. (CVE-2010-4082)
Dan Rosenberg discovered that the semctl syscall did not correctly clear kernel memory. A local attacker could exploit this to read kernel stack memory, leading to a loss of privacy. (CVE-2010-4083)
James Bottomley discovered that the ICP vortex storage array controller driver did not validate certain sizes. A local attacker on a 64bit system could exploit this to crash the kernel, leading to a denial of service. (CVE-2010-4157)
Dan Rosenberg discovered that the Linux kernel L2TP implementation contained multiple integer signedness errors. A local attacker could exploit this to to crash the kernel, or possibly gain root privileges. (CVE-2010-4160)
Steve Chen discovered that setsockopt did not correctly check MSS values. A local attacker could make a specially crafted socket call to crash the system, leading to a denial of service. (CVE-2010-4165)
Dave Jones discovered that the mprotect system call did not correctly handle merged VMAs. A local attacker could exploit this to crash the system, leading to a denial of service. (CVE-2010-4169)
It was discovered that multithreaded exec did not handle CPU timers correctly. A local attacker could exploit this to crash the system, leading to a denial of service. (CVE-2010-4248)
Vegard Nossum discovered that memory garbage collection was not handled correctly for active sockets. A local attacker could exploit this to allocate all available kernel memory, leading to a denial of service. (CVE-2010-4249)

See Also

http://www.ubuntu.com/usn/usn-1073-1/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

References

CVE	CVE-2010-0435
CVE	CVE-2010-3448
CVE	CVE-2010-3698
CVE	CVE-2010-3859
CVE	CVE-2010-3865
CVE	CVE-2010-3873
CVE	CVE-2010-3874
CVE	CVE-2010-3875
CVE	CVE-2010-3876
CVE	CVE-2010-3877
CVE	CVE-2010-3880
CVE	CVE-2010-4074
CVE	CVE-2010-4078
CVE	CVE-2010-4079
CVE	CVE-2010-4080
CVE	CVE-2010-4081
CVE	CVE-2010-4082
CVE	CVE-2010-4083
CVE	CVE-2010-4157
CVE	CVE-2010-4160
CVE	CVE-2010-4165
CVE	CVE-2010-4169
CVE	CVE-2010-4248
CVE	CVE-2010-4249
XREF	USN:1073-1

Ports

tcp/0

```
- Installed package : linux-libc-dev_2.6.31-21.59
```

```
    Fixed package     : linux-libc-dev_2.6.31-22.73
```

48381 - USN-974-1 : linux, linux-{ec2,fsl-imx51,mvl-dove,source-2.6.15,ti-omap} vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Gael Delalleu, Rafal Wojtczuk, and Brad Spengler discovered that the memory manager did not properly handle when applications grow stacks into adjacent memory regions. A local attacker could exploit this to gain control of certain applications, potentially leading to privilege escalation, as demonstrated in attacks against the X server. (CVE-2010-2240)
Kees Cook discovered that under certain situations the ioctl subsystem for DRM did not properly sanitize its arguments. A local attacker could exploit this to read previously freed kernel memory, leading to a loss of privacy. (CVE-2010-2803)
Ben Hawkes discovered an integer overflow in the Controller Area Network (CAN) subsystem when setting up frame content and filtering certain messages. An attacker could send specially crafted CAN traffic to crash the system or gain root privileges. (CVE-2010-2959)

See Also

http://www.ubuntu.com/usn/usn-974-1/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

References

CVE	CVE-2010-2240
CVE	CVE-2010-2803
CVE	CVE-2010-2959
XREF	USN:974-1

Ports

tcp/0

```
  - Installed package : linux-libc-dev_2.6.31-21.59
    Fixed package     : linux-libc-dev_2.6.31-22.63
```

50318 - USN-1009-1 : glibc, eglibc vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Tavis Ormandy discovered multiple flaws in the GNU C Library's handling of the LD_AUDIT environment variable when running a privileged binary. A local attacker could exploit this to gain root privileges. (CVE-2010-3847, CVE-2010-3856)

See Also

http://www.ubuntu.com/usn/usn-1009-1/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

References

CVE	CVE-2010-3847
CVE	CVE-2010-3856
XREF	USN:1009-1

Exploitable with

CANVAS (true)

Ports

tcp/0

```
- Installed package : libc-bin_2.10.1-0ubuntu16
  Fixed package     : libc-bin_2.10.1-0ubuntu18

- Installed package : libc-dev-bin_2.10.1-0ubuntu16
  Fixed package     : libc-dev-bin_2.10.1-0ubuntu18

- Installed package : libc6_2.10.1-0ubuntu16
  Fixed package     : libc6_2.10.1-0ubuntu18

- Installed package : libc6-dev_2.10.1-0ubuntu16
  Fixed package     : libc6-dev_2.10.1-0ubuntu18

- Installed package : libc6-i686_2.10.1-0ubuntu16
  Fixed package     : libc6-i686_2.10.1-0ubuntu18
```

55067 - USN-1108-2 : dhcp3 vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

USN-1108-1 fixed vulnerabilities in DHCP. Due to an error, the patch to fix the vulnerability was not properly applied on Ubuntu 9.10 and higher. This update fixes the problem.
Original advisory details:
Sebastian Krahmer discovered that the dhclient utility incorrectly filtered crafted responses. An attacker could use this flaw with a malicious DHCP server to execute arbitrary code, resulting in root privilege escalation.

See Also

http://www.ubuntu.com/usn/usn-1108-2/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

CVE	CVE-2011-0997
XREF	USN:1108-2

Exploitable with

CANVAS (true)

Ports

tcp/0

```
- Installed package : dhcp3-client_3.1.2-1ubuntu7.1
  Fixed package     : dhcp3-client_3.1.2-1ubuntu7.3
```

49283 - USN-988-1 : linux, linux-source-2.6.15 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Ben Hawkes discovered that the Linux kernel did not correctly validate memory ranges on 64bit kernels when allocating memory on behalf of 32bit system calls. On a 64bit system, a local attacker could perform malicious multicast getsockopt calls to gain root privileges. (CVE-2010-3081)
Ben Hawkes discovered that the Linux kernel did not correctly filter registers on 64bit kernels when performing 32bit system calls. On a 64bit system, a local attacker could manipulate 32bit system calls to gain root privileges. (CVE-2010-3301)

See Also

http://www.ubuntu.com/usn/usn-988-1/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

References

CVE	CVE-2010-3081
CVE	CVE-2010-3301
XREF	USN:988-1

Ports

tcp/0

```
- Installed package : linux-libc-dev_2.6.31-21.59
  Fixed package     : linux-libc-dev_2.6.31-22.65
```

51436 - USN-1039-1 : apparmor update

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that if AppArmor was misconfigured, under certain circumstances the parser could generate policy using an unconfined fallback execute transition when one was not specified.

See Also

http://www.ubuntu.com/usn/usn-1039-1/

Solution

Update the affected package(s).

Risk Factor

High

References

XREF	USN:1039-1

Ports

tcp/0

```
- Installed package : libapparmor-perl_2.3.1+1403-0ubuntu27.3
  Fixed package     : libapparmor-perl_2.3.1+1403-0ubuntu27.4
```

```
- Installed package : libapparmor1_2.3.1+1403-0ubuntu27.3
  Fixed package     : libapparmor1_2.3.1+1403-0ubuntu27.4
```

50491 - USN-1013-1 : freetype vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Marc Schoenefeld discovered that FreeType did not correctly handle certain malformed font files. If a user were tricked into using a specially crafted font file, a remote attacker could cause FreeType to crash or possibly execute arbitrary code with user privileges.
This issue only affected Ubuntu 6.06 LTS, 8.04 LTS, 9.10 and 10.04 LTS. (CVE-2010-3311)
Chris Evans discovered that FreeType did not correctly handle certain malformed TrueType font files. If a user were tricked into using a specially crafted TrueType file, a remote attacker could cause FreeType to crash or possibly execute arbitrary code with user privileges. This issue only affected Ubuntu 8.04 LTS, 9.10, 10.04 LTS and 10.10. (CVE-2010-3814)
It was discovered that FreeType did not correctly handle certain malformed TrueType font files. If a user were tricked into using a specially crafted TrueType file, a remote attacker could cause FreeType to crash or possibly execute arbitrary code with user privileges. (CVE-2010-3855)

See Also

http://www.ubuntu.com/usn/usn-1013-1/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

CVE	CVE-2010-3311
CVE	CVE-2010-3814
CVE	CVE-2010-3855
XREF	USN:1013-1

Ports

tcp/0

```
- Installed package : libfreetype6_2.3.9-5
  Fixed package     : libfreetype6_2.3.9-5ubuntu0.4
```

50843 - USN-1023-1 : linux, linux-{ec2,source-2.6.15} vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Nelson Elhage discovered several problems with the Acorn Econet protocol driver. A local user could cause a denial of service via a NULL pointer dereference, escalate privileges by overflowing the kernel stack, and assign Econet addresses to arbitrary interfaces.

See Also

http://www.ubuntu.com/usn/usn-1023-1/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

References

CVE	CVE-2010-3848
CVE	CVE-2010-3849
CVE	CVE-2010-3850
XREF	USN:1023-1

Ports

tcp/0

```
- Installed package : linux-libc-dev_2.6.31-21.59
  Fixed package     : linux-libc-dev_2.6.31-22.69
```

53372 - USN-1108-1 : dhcp3 vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Sebastian Krahmer discovered that the dhclient utility incorrectly filtered crafted responses. An attacker could use this flaw with a malicious DHCP server to execute arbitrary code, resulting in root privilege escalation.

See Also

http://www.ubuntu.com/usn/usn-1108-1/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

CVE	CVE-2011-0997
XREF	USN:1108-1

Exploitable with

CANVAS (true)

Ports

tcp/0

```
- Installed package : dhcp3-client_3.1.2-1ubuntu7.1
  Fixed package     : dhcp3-client_3.1.2-1ubuntu7.2

- Installed package : dhcp3-common_3.1.2-1ubuntu7.1
  Fixed package     : dhcp3-common_3.1.2-1ubuntu7.2
```

48253 - USN-966-1 : linux, linux-{source-2.6.15,ec2,mvl-dove,ti-omap} vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Junjiro R. Okajima discovered that knfsd did not correctly handle strict overcommit. A local attacker could exploit this to crash knfsd, leading to a denial of service. (Only Ubuntu 6.06 LTS and 8.04 LTS were affected.) (CVE-2008-7256, CVE-2010-1643)

Chris Guo, Jukka Taimisto, and Olli Jarva discovered that SCTP did not correctly handle invalid parameters. A remote attacker could send specially crafted traffic that could crash the system, leading to a denial of service. (CVE-2010-1173)
Mario Mikocevic discovered that GFS2 did not correctly handle certain quota structures. A local attacker could exploit this to crash the system, leading to a denial of service. (Ubuntu 6.06 LTS was not affected.) (CVE-2010-1436)
Toshiyuki Okajima discovered that the kernel keyring did not correctly handle dead keyrings. A local attacker could exploit this to crash the system, leading to a denial of service. (CVE-2010-1437)
Brad Spengler discovered that Sparc did not correctly implement non-executable stacks. This made userspace applications vulnerable to exploits that would have been otherwise blocked due to non-executable memory protections. (Ubuntu 10.04 LTS was not affected.) (CVE-2010-1451)
Dan Rosenberg discovered that the btrfs clone function did not correctly validate permissions. A local attacker could exploit this to read sensitive information, leading to a loss of privacy. (Only Ubuntu 9.10 was affected.) (CVE-2010-1636)
Dan Rosenberg discovered that GFS2 set_flags function did not correctly validate permissions. A local attacker could exploit this to gain access to files, leading to a loss of privacy and potential privilege escalation. (Ubuntu 6.06 LTS was not affected.) (CVE-2010-1641)
Shi Weihua discovered that btrfs xattr_set_acl function did not correctly validate permissions. A local attacker could exploit this to gain access to files, leading to a loss of privacy and potential privilege escalation. (Only Ubuntu 9.10 and 10.04 LTS were affected.) (CVE-2010-2071)
Andre Osterhues discovered that eCryptfs did not correctly calculate hash values. A local attacker with certain uids could exploit this to crash the system or potentially gain root privileges. (Ubuntu 6.06 LTS was not affected.) (CVE-2010-2492)

See Also

http://www.ubuntu.com/usn/usn-966-1/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

7.1 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:C)

References

CVE	CVE-2008-7256
CVE	CVE-2010-1173
CVE	CVE-2010-1436
CVE	CVE-2010-1437
CVE	CVE-2010-1451
CVE	CVE-2010-1636
CVE	CVE-2010-1641
CVE	CVE-2010-1643
CVE	CVE-2010-2071
CVE	CVE-2010-2492
XREF	USN:966-1

Ports

tcp/0

```
  - Installed package : linux-libc-dev_2.6.31-21.59
    Fixed package     : linux-libc-dev_2.6.31-22.61
```

47778 - USN-963-1 : freetype vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Robert #wi#cki discovered that FreeType did not correctly handle certain malformed font files. If a user were tricked into using a specially crafted font file, a remote attacker could execute arbitrary code with user privileges.

See Also

http://www.ubuntu.com/usn/usn-963-1/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

CVE	CVE-2010-2498
CVE	CVE-2010-2499
CVE	CVE-2010-2500
CVE	CVE-2010-2519
CVE	CVE-2010-2520
CVE	CVE-2010-2527
XREF	OSVDB:66462
XREF	OSVDB:66463
XREF	OSVDB:66464
XREF	OSVDB:66465
XREF	OSVDB:66466
XREF	OSVDB:66467
XREF	USN:963-1

Ports

tcp/0

```
  - Installed package : libfreetype6_2.3.9-5
    Fixed package     : libfreetype6_2.3.9-5ubuntu0.1
```

48361 - USN-972-1 : freetype vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that FreeType did not correctly handle certain malformed font files. If a user were tricked into using a specially crafted font file, a remote attacker could cause FreeType to crash or possibly execute arbitrary code with user privileges.

See Also

http://www.ubuntu.com/usn/usn-972-1/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

References

CVE	CVE-2010-1797
CVE	CVE-2010-2541
CVE	CVE-2010-2805
CVE	CVE-2010-2806
CVE	CVE-2010-2807
CVE	CVE-2010-2808
XREF	OSVDB:67011
XREF	OSVDB:67301
XREF	OSVDB:67302
XREF	OSVDB:67303
XREF	OSVDB:67304
XREF	OSVDB:67305
XREF	USN:972-1

Exploitable with

CANVAS (true)Core Impact (true)

Ports

tcp/0

```
  - Installed package : libfreetype6_2.3.9-5
    Fixed package     : libfreetype6_2.3.9-5ubuntu0.2
```

46731 - USN-944-1 : glibc, eglibc vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Maksymilian Arciemowicz discovered that the GNU C library did not correctly handle integer overflows in the strfmon function. If a user or automated system were tricked into processing a specially crafted format string, a remote attacker could crash applications, leading to a denial of service. (Ubuntu 10.04 was not affected.) (CVE-2008-1391)
Jeff Layton and Dan Rosenberg discovered that the GNU C library did not correctly handle newlines in the mntent family of functions. If a local attacker were able to inject newlines into a mount entry through other vulnerable mount helpers, they could disrupt the system or possibly gain root privileges. (CVE-2010-0296)
Dan Rosenberg discovered that the GNU C library did not correctly validate certain ELF program headers. If a user or automated system were tricked into verifying a specially crafted ELF program, a remote attacker could execute arbitrary code with user privileges.
(CVE-2010-0830)

See Also

http://www.ubuntu.com/usn/usn-944-1/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

CVE	CVE-2008-1391
CVE	CVE-2010-0296
CVE	CVE-2010-0830
XREF	OSVDB:65077
XREF	OSVDB:65078
XREF	OSVDB:65080
XREF	USN:944-1
XREF	CWE:189

Ports

tcp/0

```
- Installed package : libc-bin_2.10.1-0ubuntu16
  Fixed package     : libc-bin_2.10.1-0ubuntu17

- Installed package : libc-dev-bin_2.10.1-0ubuntu16
  Fixed package     : libc-dev-bin_2.10.1-0ubuntu17

- Installed package : libc6_2.10.1-0ubuntu16
  Fixed package     : libc6_2.10.1-0ubuntu17

- Installed package : libc6-dev_2.10.1-0ubuntu16
  Fixed package     : libc6-dev_2.10.1-0ubuntu17

- Installed package : libc6-i686_2.10.1-0ubuntu16
  Fixed package     : libc6-i686_2.10.1-0ubuntu17
```

50649 - USN-1018-1 : openssl vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Rob Hulswit discovered a race condition in the OpenSSL TLS server extension parsing code when used within a threaded server. A remote attacker could trigger this flaw to cause a denial of service or possibly execute arbitrary code with application privileges.
(CVE-2010-3864)

See Also

http://www.ubuntu.com/usn/usn-1018-1/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

References

CVE	CVE-2010-3864
XREF	IAVA:2010-A-0166
XREF	USN:1018-1

Ports

tcp/0

```
- Installed package : libssl0.9.8_0.9.8g-16ubuntu3.1
  Fixed package     : libssl0.9.8_0.9.8g-16ubuntu3.4

- Installed package : openssl_0.9.8g-16ubuntu3.1
  Fixed package     : openssl_0.9.8g-16ubuntu3.4
```

51501 - USN-1009-2 : eglibc, glibc vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

USN-1009-1 fixed vulnerabilities in the GNU C library. Colin Watson discovered that the fixes were incomplete and introduced flaws with setuid programs loading libraries that used dynamic string tokens in their RPATH. If the 'man' program was installed setuid, a local attacker could exploit this to gain 'man' user privileges, potentially leading to further privilege escalations. Default Ubuntu installations were not affected.
Original advisory details:
Tavis Ormandy discovered multiple flaws in the GNU C Library's handling of the LD_AUDIT environment variable when running a privileged binary. A local attacker could exploit this to gain root privileges. (CVE-2010-3847, CVE-2010-3856)

See Also

http://www.ubuntu.com/usn/usn-1009-2/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

References

CVE	CVE-2010-3847
CVE	CVE-2010-3856
XREF	USN:1009-2

Exploitable with

CANVAS (true)

Ports

tcp/0

```
- Installed package : libc-bin_2.10.1-0ubuntu16
  Fixed package     : libc-bin_2.10.1-0ubuntu19

- Installed package : libc-dev-bin_2.10.1-0ubuntu16
  Fixed package     : libc-dev-bin_2.10.1-0ubuntu19

- Installed package : libc6_2.10.1-0ubuntu16
  Fixed package     : libc6_2.10.1-0ubuntu19

- Installed package : libc6-dev_2.10.1-0ubuntu16
  Fixed package     : libc6-dev_2.10.1-0ubuntu19
```

```
- Installed package : libc6-i686_2.10.1-0ubuntu16
  Fixed package     : libc6-i686_2.10.1-0ubuntu19
```

55086 - USN-1126-1 : php5 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Stephane Chazelas discovered that the /etc/cron.d/php5 cron job for PHP 5.3.5 allows local users to delete arbitrary files via a symlink attack on a directory under /var/lib/php5/. (CVE-2011-0441)
Raphael Geisert and Dan Rosenberg discovered that the PEAR installer allows local users to overwrite arbitrary files via a symlink attack on the package.xml file, related to the (1) download_dir, (2) cache_dir, (3) tmp_dir, and (4) pear-build-download directories.
(CVE-2011-1072, CVE-2011-1144)
Ben Schmidt discovered that a use-after-free vulnerability in the PHP Zend engine could allow an attacker to cause a denial of service (heap memory corruption) or possibly execute arbitrary code.
(CVE-2010-4697)
Martin Barbella discovered a buffer overflow in the PHP GD extension that allows an attacker to cause a denial of service (application crash) via a large number of anti- aliasing steps in an argument to the imagepstext function.
(CVE-2010-4698)
It was discovered that PHP accepts the \0 character in a pathname, which might allow an attacker to bypass intended access restrictions by placing a safe file extension after this character. This issue is addressed in Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04.
(CVE-2006-7243)
Maksymilian Arciemowicz discovered that the grapheme_extract function in the PHP Internationalization extension (Intl) for ICU allow an attacker to cause a denial of service (crash) via an invalid size argument, which triggers a NULL pointer dereference. This issue affected Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04.
(CVE-2011-0420)
Maksymilian Arciemowicz discovered that the _zip_name_locate function in the PHP Zip extension does not properly handle a ZIPARCHIVE::FL_UNCHANGED argument, which might allow an attacker to cause a denial of service (NULL pointer dereference) via an empty ZIP archive. This issue affected Ubuntu 8.04 LTS, Ubuntu 9.10, Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04. (CVE-2011-0421)
Luca Carettoni discovered that the PHP Exif extension performs an incorrect cast on 64bit platforms, which allows a remote attacker to cause a denial of service (application crash) via an image with a crafted Image File Directory (IFD).
(CVE-2011-0708)
Jose Carlos Norte discovered that an integer overflow in the PHP shmop extension could allow an attacker to cause a denial of service (crash) and possibly read sensitive memory function. (CVE-2011-1092)
Felipe Pena discovered that a use-after-free vulnerability in the substr_replace function allows an attacker to cause a denial of service (memory corruption) or possibly execute arbitrary code.
(CVE-2011-1148)
Felipe Pena discovered multiple format string vulnerabilities in the PHP phar extension. These could allow an attacker to obtain sensitive information from process memory, cause a denial of service (memory corruption), or possibly execute arbitrary code. This issue affected Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04.(CVE-2011-1153)
It was discovered that a buffer overflow occurs in the strval function when the precision configuration option has a large value.
The default compiler options for Ubuntu 8.04 LTS, Ubuntu 9.10, Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04 should reduce the vulnerability to a denial of service. (CVE-2011-1464)
It was discovered that an integer overflow in the SdnToJulian function in the PHP Calendar extension could allow an attacker to cause a denial of service (application crash). (CVE-2011-1466)
Tomas Hoger discovered that an integer overflow in the NumberFormatter::setSymbol function in the PHP Intl extension could allow an attacker to cause a denial of service (application crash).
This issue affected Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04.
(CVE-2011-1467)
It was discovered that multiple memory leaks in the PHP OpenSSL extension might allow a remote attacker to cause a denial of service (memory consumption). This issue affected Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04.
(CVE-2011-1468)
Daniel Buschke discovered that the PHP Streams component in PHP handled types improperly, possibly allowing an attacker to cause a denial of service (application crash). (CVE-2011-1469)
It was discovered that the PHP Zip extension could allow an attacker to cause a denial of service (application crash) via a ziparchive stream that is not properly handled by the stream_get_contents function. This issue affected Ubuntu 8.04 LTS, Ubuntu 9.10, Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04. (CVE-2011-1470)
It was discovered that an integer signedness error in the PHP Zip extension could allow an attacker to cause a denial of service (CPU consumption) via a malformed archive file. This issue affected Ubuntu 8.04 LTS, Ubuntu 9.10, Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04. (CVE-2011-1470) (CVE-2011-1471)

See Also

http://www.ubuntu.com/usn/usn-1126-1/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

CVE	CVE-2006-7243
CVE	CVE-2010-4697
CVE	CVE-2010-4698
CVE	CVE-2011-0420
CVE	CVE-2011-0421
CVE	CVE-2011-0441
CVE	CVE-2011-0708
CVE	CVE-2011-1072
CVE	CVE-2011-1092
CVE	CVE-2011-1144
CVE	CVE-2011-1148
CVE	CVE-2011-1153
CVE	CVE-2011-1464
CVE	CVE-2011-1466
CVE	CVE-2011-1467
CVE	CVE-2011-1468
CVE	CVE-2011-1469
CVE	CVE-2011-1470
CVE	CVE-2011-1471
XREF	USN:1126-1

Ports

tcp/0

```
  - Installed package : libapache2-mod-php5_5.2.10.dfsg.1-2ubuntu6.4
    Fixed package     : libapache2-mod-php5_5.2.10.dfsg.1-2ubuntu6.9

  - Installed package : php5_5.2.10.dfsg.1-2ubuntu6.4
    Fixed package     : php5_5.2.10.dfsg.1-2ubuntu6.9

  - Installed package : php5-common_5.2.10.dfsg.1-2ubuntu6.4
    Fixed package     : php5-common_5.2.10.dfsg.1-2ubuntu6.9
```

55087 - USN-1126-2 : php5 regressions

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

USN 1126-1 fixed several vulnerabilities in PHP. The fix for CVE-2010-4697 introduced an incorrect reference counting regression in the Zend engine that caused the PHP interpreter to segfault. This regression affects Ubuntu 6.06 LTS and Ubuntu 8.04 LTS.
The fixes for CVE-2011-1072 and CVE-2011-1144 introduced a regression in the PEAR installer that prevented it from creating its cache directory and reporting errors correctly.
We apologize for the inconvenience.
Original advisory details:
Stephane Chazelas discovered that the /etc/cron.d/php5 cron job for PHP 5.3.5 allows local users to delete arbitrary files via a symlink attack on a directory under /var/lib/php5/. (CVE-2011-0441) Raphael Geisert and Dan Rosenberg discovered that the PEAR installer allows local users to overwrite arbitrary files via a symlink attack on the package.xml file, related to the (1) download_dir, (2) cache_dir, (3) tmp_dir, and (4) pear-build-download directories. (CVE-2011-1072, CVE-2011-1144) Ben Schmidt discovered that a use-after-free vulnerability in the PHP Zend engine could allow an attacker to cause a denial of service (heap memory corruption) or possibly execute arbitrary code. (CVE-2010-4697) Martin Barbella discovered a buffer overflow in the PHP GD extension that allows an attacker to cause a denial of service (application crash) via a large number of anti- aliasing steps in an argument to the imagepstext function. (CVE-2010-4698) It was discovered that PHP accepts the \0 character in a pathname, which might allow an attacker to bypass intended access restrictions by placing a safe file extension after this character. This issue is addressed in Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04.
(CVE-2006-7243) Maksymilian Arciemowicz discovered that the grapheme_extract function in the PHP Internationalization extension (Intl) for ICU allow an attacker to cause a denial of service (crash) via an invalid size argument, which triggers a NULL pointer dereference. This issue affected Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04.
(CVE-2011-0420) Maksymilian Arciemowicz discovered that the _zip_name_locate function in the PHP Zip extension does not properly handle a ZIPARCHIVE::FL_UNCHANGED argument, which might allow an attacker to cause a denial of service (NULL pointer dereference) via an empty ZIP archive. This issue affected Ubuntu 8.04 LTS, Ubuntu 9.10, Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04. (CVE-2011-0421) Luca Carettoni discovered that the PHP Exif extension performs an incorrect cast on 64bit platforms, which allows a remote attacker to cause a denial of service (application crash) via an image with a crafted Image File Directory (IFD). (CVE-2011-0708) Jose Carlos Norte discovered that an integer overflow in the PHP shmop extension could allow an attacker to cause a denial of service (crash) and possibly read sensitive memory function. (CVE-2011-1092) Felipe Pena discovered that a use-after-free vulnerability in the substr_replace function allows an attacker to cause a denial of service (memory corruption) or possibly execute arbitrary code.
(CVE-2011-1148) Felipe Pena discovered multiple format string vulnerabilities in the PHP phar extension. These could allow an attacker to obtain sensitive information from process memory, cause a denial of service (memory corruption), or possibly execute arbitrary code. This issue affected Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04.(CVE-2011-1153) It was discovered that a buffer overflow occurs in the strval function when the precision configuration option has a large value.
The default compiler options for Ubuntu 8.04 LTS, Ubuntu 9.10, Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04 should reduce the vulnerability to a denial of service. (CVE-2011-1464) It was discovered that an integer overflow in the SdnToJulian function in the PHP Calendar extension could allow an attacker to cause a denial of service (application crash). (CVE-2011-1466) Tomas Hoger discovered that an integer overflow in the NumberFormatter::setSymbol function in the PHP Intl extension could allow an attacker to cause a denial of service (application crash).
This issue affected Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04.
(CVE-2011-1467) It was discovered that multiple memory leaks in the PHP OpenSSL extension might allow a remote attacker to cause a denial of service (memory consumption). This issue affected Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04. (CVE-2011-1468) Daniel Buschke discovered that the PHP Streams component in PHP handled types improperly, possibly allowing an attacker to cause a denial of service (application crash). (CVE-2011-1469) It was discovered that the PHP Zip extension could allow an attacker to cause a denial of service (application crash) via a ziparchive stream that is not properly handled by the stream_get_contents function. This issue affected Ubuntu 8.04 LTS, Ubuntu 9.10, Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04. (CVE-2011-1470) It was discovered that an integer signedness error in the PHP Zip extension could allow an attacker to cause a denial of service (CPU consumption) via a malformed archive file. This issue affected Ubuntu 8.04 LTS, Ubuntu 9.10, Ubuntu 10.04 LTS, Ubuntu 10.10, and Ubuntu 11.04. (CVE-2011-1470) (CVE-2011-1471)

See Also

http://www.ubuntu.com/usn/usn-1126-2/

Solution

Update the affected package(s).

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

CVE	CVE-2006-7243
CVE	CVE-2010-4697
CVE	CVE-2010-4698
CVE	CVE-2011-0420
CVE	CVE-2011-0421
CVE	CVE-2011-0441
CVE	CVE-2011-0708
CVE	CVE-2011-1072
CVE	CVE-2011-1092
CVE	CVE-2011-1144
CVE	CVE-2011-1148
CVE	CVE-2011-1153
CVE	CVE-2011-1464
CVE	CVE-2011-1466
CVE	CVE-2011-1467
CVE	CVE-2011-1468
CVE	CVE-2011-1469
CVE	CVE-2011-1470
CVE	CVE-2011-1471
XREF	USN:1126-2

Ports

tcp/0

```
- Installed package : libapache2-mod-php5_5.2.10.dfsg.1-2ubuntu6.4
  Fixed package     : libapache2-mod-php5_5.2.10.dfsg.1-2ubuntu6.10

- Installed package : php5_5.2.10.dfsg.1-2ubuntu6.4
  Fixed package     : php5_5.2.10.dfsg.1-2ubuntu6.10

- Installed package : php5-common_5.2.10.dfsg.1-2ubuntu6.4
  Fixed package     : php5-common_5.2.10.dfsg.1-2ubuntu6.10
```

55071 - USN-1113-1 : postfix vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that the Postfix package incorrectly granted write access on the PID directory to the postfix user. A local attacker could use this flaw to possibly conduct a symlink attack and overwrite arbitrary files. This issue only affected Ubuntu 6.06 LTS and 8.04 LTS. (CVE-2009-2939)
Wietse Venema discovered that Postfix incorrectly handled cleartext commands after TLS is in place. A remote attacker could exploit this to inject cleartext commands into TLS sessions, and possibly obtain confidential information such as passwords. (CVE-2011-0411)

See Also

http://www.ubuntu.com/usn/usn-1113-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

6.9 (CVSS2#AV:L/AC:M/Au:N/C:C/I:C/A:C)

References

CVE	CVE-2009-2939
CVE	CVE-2011-0411
XREF	IAVA:2011-A-0054
XREF	USN:1113-1
XREF	CWE:59

Ports

tcp/0

```
- Installed package : postfix_2.6.5-3
  Fixed package     : postfix_2.6.5-3ubuntu0.1
```

48283 - USN-967-1 : w3m vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Ludwig Nussel discovered w3m does not properly handle SSL/TLS certificates with NULL characters in the certificate name. An attacker could exploit this to perform a man in the middle attack to view sensitive information or alter encrypted communications.
(CVE-2010-2074)

See Also

http://www.ubuntu.com/usn/usn-967-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

References

CVE	CVE-2010-2074
XREF	OSVDB:65538
XREF	USN:967-1

Ports
tcp/0

```
  - Installed package : w3m_0.5.2-2ubuntu1
    Fixed package     : w3m_0.5.2-2ubuntu1.1
```

49066 - USN-981-1 : libwww-perl vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that libwww-perl incorrectly filtered filenames suggested by Content-Disposition headers. If a user were tricked into downloading a file from a malicious site, a remote attacker could overwrite hidden files in the user's directory.

See Also

http://www.ubuntu.com/usn/usn-981-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

References

CVE	CVE-2010-2253
XREF	USN:981-1

Ports
tcp/0

```
  - Installed package : libwww-perl_5.831-1
    Fixed package     : libwww-perl_5.831-1ubuntu0.1
```

49644 - USN-990-2 : apache2 vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

USN-860-1 introduced a partial workaround to Apache that disabled client initiated TLS renegotiation in order to mitigate CVE-2009-3555. USN-990-1 introduced the new RFC5746 renegotiation extension in openssl, and completely resolves the issue.
After updating openssl, an Apache server will allow both patched and unpatched web browsers to connect, but unpatched browsers will not be able to renegotiate. This update introduces the new SSLInsecureRenegotiation directive for Apache that may be used to re-enable insecure renegotiations with unpatched web browsers. For more information, please refer to:
http://httpd.apache.org/docs/2.2/mod/mod_ssl.html#sslinsecurerenegoti ation
Original advisory details:
Marsh Ray and Steve Dispensa discovered a flaw in the TLS and SSLv3 protocols. If an attacker could perform a man in the middle attack at the start of a TLS connection, the attacker could inject arbitrary content at the beginning of the user's session. This update adds backported support for the new RFC5746 renegotiation extension and will use it when both the client and the server support it.

See Also

http://www.ubuntu.com/usn/usn-990-2/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:P)

References

CVE	CVE-2009-3555
XREF	OSVDB:59969
XREF	IAVA:2009-A-0122
XREF	IAVA:2010-A-0047
XREF	IAVA:2010-A-0048
XREF	IAVA:2010-A-0072
XREF	IAVA:2010-A-0089
XREF	IAVA:2010-A-0108
XREF	IAVA:2010-A-0149
XREF	IAVA:2010-A-0155
XREF	IAVA:2011-A-0007
XREF	IAVA:2011-A-0055
XREF	IAVA:2011-A-0058
XREF	IAVA:2011-A-0107
XREF	USN:990-2
XREF	CWE:310

Ports

tcp/0

```
  - Installed package : apache2_2.2.12-1ubuntu2.2
    Fixed package     : apache2_2.2.12-1ubuntu2.3

  - Installed package : apache2-mpm-prefork_2.2.12-1ubuntu2.2
    Fixed package     : apache2-mpm-prefork_2.2.12-1ubuntu2.3

  - Installed package : apache2-utils_2.2.12-1ubuntu2.2
    Fixed package     : apache2-utils_2.2.12-1ubuntu2.3

  - Installed package : apache2.2-bin_2.2.12-1ubuntu2.2
    Fixed package     : apache2.2-bin_2.2.12-1ubuntu2.3

  - Installed package : apache2.2-common_2.2.12-1ubuntu2.2
    Fixed package     : apache2.2-common_2.2.12-1ubuntu2.3
```

50560 - USN-1016-1 : libxml2 vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Bui Quang Minh discovered that libxml2 did not properly process XPath namespaces and attributes. If an application using libxml2 opened a specially crafted XML file, an attacker could cause a denial of service or possibly execute code as the user invoking the program.

See Also

http://www.ubuntu.com/usn/usn-1016-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)

References

CVE	CVE-2010-4008
XREF	USN:1016-1

Ports

tcp/0

```
- Installed package : libxml2_2.7.5.dfsg-1ubuntu1.1
  Fixed package     : libxml2_2.7.5.dfsg-1ubuntu1.2
```

51435 - USN-1038-1 : dpkg vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Jakub Wilk and Raphaël Hertzog discovered that dpkg-source did not correctly handle certain paths and symlinks when unpacking source-format version 3.0 packages. If a user or an automated system were tricked into unpacking a specially crafted source package, a remote attacker could modify files outside the target unpack directory, leading to a denial of service or potentially gaining access to the system.

See Also

http://www.ubuntu.com/usn/usn-1038-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

References

CVE	CVE-2010-1679
XREF	USN:1038-1

Ports

tcp/0

```
- Installed package : dpkg_1.15.4ubuntu2.1
  Fixed package     : dpkg_1.15.4ubuntu2.3

- Installed package : dpkg-dev_1.15.4ubuntu2.1
  Fixed package     : dpkg-dev_1.15.4ubuntu2.3
```

55085 - USN-1125-1 : pcsc-lite vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Rafael Dominguez Vega discovered that PCSC-Lite incorrectly handled smart cards with malformed ATR messages. An attacker having physical access could exploit this with a special smart card and cause a denial of service or execute arbitrary code.

See Also

http://www.ubuntu.com/usn/usn-1125-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

4.4 (CVSS2#AV:L/AC:M/Au:N/C:P/I:P/A:P)

References

CVE	CVE-2010-4531
XREF	USN:1125-1

Ports

tcp/0

```
- Installed package : libpcsclite1_1.5.3-1ubuntu1
  Fixed package     : libpcsclite1_1.5.3-1ubuntu1.2
```

49303 - USN-986-1 : bzip2 vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

An integer overflow was discovered in bzip2. If a user or automated system were tricked into decompressing a crafted bz2 file, an attacker could cause bzip2 or any application linked against libbz2 to crash or possibly execute code as the user running the program.

See Also

http://www.ubuntu.com/usn/usn-986-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

References

CVE	CVE-2010-0405
XREF	OSVDB:68167
XREF	USN:986-1

Ports

tcp/0

```
- Installed package : bzip2_1.0.5-3
  Fixed package     : bzip2_1.0.5-3ubuntu0.1

- Installed package : libbz2-1.0_1.0.5-3
  Fixed package     : libbz2-1.0_1.0.5-3ubuntu0.1
```

51643 - USN-1046-1 : sudo vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Alexander Kurtz discovered that sudo would not prompt for a password when a group was specified in the Runas_Spec. A local attacker could exploit this to execute arbitrary code as the specified group if sudo was configured to allow the attacker to use a program as this group.
The group Runas_Spec is not used in the default installation of Ubuntu.

See Also

http://www.ubuntu.com/usn/usn-1046-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

4.4 (CVSS2#AV:L/AC:M/Au:N/C:P/I:P/A:P)

References

CVE	CVE-2011-0010
XREF	USN:1046-1

Ports

tcp/0

```
- Installed package : sudo_1.7.0-1ubuntu2.2
  Fixed package     : sudo_1.7.0-1ubuntu2.6
```

48262 - USN-969-1 : pcsc-lite vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that the PC/SC service did not correctly handle malformed messages. A local attacker could exploit this to execute arbitrary code with root privileges.

See Also

http://www.ubuntu.com/usn/usn-969-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

6.8 (CVSS2#AV:L/AC:L/Au:S/C:C/I:C/A:C)

References

CVE	CVE-2009-4901
CVE	CVE-2009-4902
CVE	CVE-2010-0407
XREF	USN:969-1

Ports

tcp/0

```
- Installed package : libpcsclite1_1.5.3-1ubuntu1
  Fixed package     : libpcsclite1_1.5.3-1ubuntu1.1
```

53257 - USN-1100-1 : openldap, openldap2.3 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that OpenLDAP did not properly check forwarded authentication failures when using a slave server and chain overlay.
If OpenLDAP were configured in this manner, an attacker could bypass authentication checks by sending an invalid password to a slave server. (CVE-2011-1024)
It was discovered that OpenLDAP did not properly perform authentication checks to the rootdn when using the back-ndb backend.
An attacker could exploit this to access the directory by sending an arbitrary password. Ubuntu does not ship OpenLDAP with back-ndb support by default. This issue did not affect Ubuntu 8.04 LTS.
(CVE-2011-1025)
It was discovered that OpenLDAP did not properly validate modrdn requests. An unauthenticated remote user could use this to cause a denial of service via application crash. (CVE-2011-1081)

See Also

http://www.ubuntu.com/usn/usn-1100-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

References

CVE	CVE-2011-1024
CVE	CVE-2011-1025
CVE	CVE-2011-1081
XREF	USN:1100-1

Ports

tcp/0

```
- Installed package : libldap-2.4-2_2.4.18-0ubuntu1
  Fixed package     : libldap-2.4-2_2.4.18-0ubuntu1.2
```

49643 - USN-990-1 : openssl vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Marsh Ray and Steve Dispensa discovered a flaw in the TLS and SSLv3 protocols. If an attacker could perform a man in the middle attack at the start of a TLS connection, the attacker could inject arbitrary content at the beginning of the user's session. This update adds backported support for the new RFC5746 renegotiation extension and will use it when both the client and the server support it.
ATTENTION: After applying this update, a patched server will allow both patched and unpatched clients to connect, but unpatched clients will not be able to renegotiate. For more information, please refer to the following:
http://www.openssl.org/docs/ssl/SSL_CTX_set_options.html#SECURE_RENEG OTIATION

See Also

http://www.ubuntu.com/usn/usn-990-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:P)

References

CVE	CVE-2009-3555
XREF	OSVDB:59971
XREF	IAVA:2009-A-0122
XREF	IAVA:2010-A-0047
XREF	IAVA:2010-A-0048
XREF	IAVA:2010-A-0072
XREF	IAVA:2010-A-0089
XREF	IAVA:2010-A-0108
XREF	IAVA:2010-A-0149
XREF	IAVA:2010-A-0155
XREF	IAVA:2011-A-0007
XREF	IAVA:2011-A-0055
XREF	IAVA:2011-A-0058
XREF	IAVA:2011-A-0107
XREF	USN:990-1
XREF	CWE:310

Ports

tcp/0

```
  - Installed package : libssl0.9.8_0.9.8g-16ubuntu3.1
    Fixed package     : libssl0.9.8_0.9.8g-16ubuntu3.2

  - Installed package : openssl_0.9.8g-16ubuntu3.1
    Fixed package     : openssl_0.9.8g-16ubuntu3.2
```

50823 - USN-1021-1 : apache2 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that Apache's mod_cache and mod_dav modules incorrectly handled requests that lacked a path. A remote attacker could exploit this with a crafted request and cause a denial of service. This issue affected Ubuntu 6.06 LTS, 8.04 LTS, 9.10 and 10.04 LTS. (CVE-2010-1452)
It was discovered that Apache did not properly handle memory when destroying APR buckets. A remote attacker could exploit this with crafted requests and cause a denial of service via memory exhaustion.
This issue affected Ubuntu 6.06 LTS and 10.10. (CVE-2010-1623)

See Also

http://www.ubuntu.com/usn/usn-1021-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

References

CVE	CVE-2010-1452
CVE	CVE-2010-1623
XREF	IAVA:2010-A-0099
XREF	USN:1021-1

Ports

tcp/0

```
- Installed package : apache2_2.2.12-1ubuntu2.2
  Fixed package     : apache2_2.2.12-1ubuntu2.4

- Installed package : apache2-mpm-prefork_2.2.12-1ubuntu2.2
  Fixed package     : apache2-mpm-prefork_2.2.12-1ubuntu2.4

- Installed package : apache2-utils_2.2.12-1ubuntu2.2
  Fixed package     : apache2-utils_2.2.12-1ubuntu2.4

- Installed package : apache2.2-bin_2.2.12-1ubuntu2.2
  Fixed package     : apache2.2-bin_2.2.12-1ubuntu2.4

- Installed package : apache2.2-common_2.2.12-1ubuntu2.2
  Fixed package     : apache2.2-common_2.2.12-1ubuntu2.4
```

51583 - USN-1045-1 : fuse vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that FUSE could be tricked into incorrectly updating the mtab file when mounting filesystems. A local attacker, with access to use FUSE, could unmount arbitrary locations, leading to a denial of service.

See Also

http://www.ubuntu.com/usn/usn-1045-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:P)

References

CVE	CVE-2010-3879
XREF	USN:1045-1

Ports

tcp/0

```
- Installed package : fuse-utils_2.7.4-1.1ubuntu4.3
  Fixed package     : fuse-utils_2.7.4-1.1ubuntu4.4

- Installed package : libfuse2_2.7.4-1.1ubuntu4.3
  Fixed package     : libfuse2_2.7.4-1.1ubuntu4.4
```

52739 - USN-1089-1 : linux, linux-ec2 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Dan Rosenberg discovered that multiple terminal ioctls did not correctly initialize structure memory. A local attacker could exploit this to read portions of kernel stack memory, leading to a loss of privacy. (CVE-2010-4076, CVE-2010-4077)
Dan Rosenberg discovered that the socket filters did not correctly initialize structure memory. A local attacker could create malicious filters to read portions of kernel stack memory, leading to a loss of privacy. (CVE-2010-4158)
Dan Rosenberg discovered that certain iovec operations did not calculate page counts correctly. A local attacker could exploit this to crash the system, leading to a denial of service. (CVE-2010-4162)
Dan Rosenberg discovered that the SCSI subsystem did not correctly validate iov segments. A local attacker with access to a SCSI device could send specially crafted requests to crash the system, leading to a denial of service. (CVE-2010-4163)
Dan Rosenberg discovered that the RDS protocol did not correctly check ioctl arguments. A local attacker could exploit this to crash the system, leading to a denial of service. (CVE-2010-4175)
Alan Cox discovered that the HCI UART driver did not correctly check if a write operation was available. If the mmap_min-addr sysctl was changed from the Ubuntu default to a value of 0, a local attacker could exploit this flaw to gain root privileges. (CVE-2010-4242)

See Also

http://www.ubuntu.com/usn/usn-1089-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

4.9 (CVSS2#AV:L/AC:L/Au:N/C:N/I:N/A:C)

References

CVE	CVE-2010-4076
CVE	CVE-2010-4077
CVE	CVE-2010-4158
CVE	CVE-2010-4162
CVE	CVE-2010-4163
CVE	CVE-2010-4175
CVE	CVE-2010-4242
XREF	USN:1089-1

Ports

tcp/0

```
- Installed package : linux-libc-dev_2.6.31-21.59
  Fixed package     : linux-libc-dev_2.6.31-23.74
```

50573 - USN-1017-1 : mysql-5.1, mysql-dfsg-5.0, mysql-dfsg-5.1 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that MySQL incorrectly handled certain requests with the UPGRADE DATA DIRECTORY NAME command. An authenticated user could exploit this to make MySQL crash, causing a denial of service.
This issue only affected Ubuntu 9.10 and 10.04 LTS. (CVE-2010-2008)
It was discovered that MySQL incorrectly handled joins involving a table with a unique SET column. An authenticated user could exploit this to make MySQL crash, causing a denial of service. This issue only affected Ubuntu 6.06 LTS, 8.04 LTS, 9.10 and 10.04 LTS.
(CVE-2010-3677)
It was discovered that MySQL incorrectly handled NULL arguments to IN() or CASE operations. An authenticated user could exploit this to make MySQL crash, causing a denial of service. This issue only affected Ubuntu 9.10 and 10.04 LTS. (CVE-2010-3678)
It was discovered that MySQL incorrectly handled malformed arguments to the BINLOG statement. An authenticated user could exploit this to make MySQL crash, causing a denial of service. This issue only affected Ubuntu 9.10 and 10.04 LTS. (CVE-2010-3679)
It was discovered that MySQL incorrectly handled the use of TEMPORARY InnoDB tables with nullable columns. An authenticated user could exploit this to make MySQL crash, causing a denial of service. This issue only affected Ubuntu 6.06 LTS, 8.04 LTS, 9.10 and 10.04 LTS.
(CVE-2010-3680)
It was discovered that MySQL incorrectly handled alternate reads from two indexes on a table using the HANDLER interface. An authenticated user could exploit this to make MySQL crash, causing a denial of service. This issue only affected Ubuntu 6.06 LTS, 8.04 LTS, 9.10 and 10.04 LTS. (CVE-2010-3681)
It was discovered that MySQL incorrectly handled use of EXPLAIN with certain queries. An authenticated user could exploit this to make MySQL crash, causing a denial of service. This issue only affected Ubuntu 6.06 LTS, 8.04 LTS, 9.10 and 10.04 LTS. (CVE-2010-3682)
It was discovered that MySQL incorrectly handled error reporting when using LOAD DATA INFILE and would incorrectly raise an assert in certain circumstances. An authenticated user could exploit this to make MySQL crash, causing a denial of service. This issue only affected Ubuntu 9.10 and 10.04 LTS. (CVE-2010-3683)
It was discovered that MySQL incorrectly handled propagation during evaluation of arguments to extreme-value functions. An authenticated user could exploit this to make MySQL crash, causing a denial of service. This issue only affected Ubuntu 8.04 LTS, 9.10, 10.04 LTS and 10.10. (CVE-2010-3833)
It was discovered that MySQL incorrectly handled materializing a derived table that required a temporary table for grouping. An authenticated user could exploit this to make MySQL crash, causing a denial of service.
(CVE-2010-3834)
It was discovered that MySQL incorrectly handled certain user-variable assignment expressions that are evaluated in a logical expression context. An authenticated user could exploit this to make MySQL crash, causing a denial of service. This issue only affected Ubuntu 8.04 LTS, 9.10, 10.04 LTS and 10.10. (CVE-2010-3835)
It was discovered that MySQL incorrectly handled pre-evaluation of LIKE predicates during view preparation. An authenticated user could exploit this to make MySQL crash, causing a denial of service.
(CVE-2010-3836)
It was discovered that MySQL incorrectly handled using GROUP_CONCAT() and WITH ROLLUP together. An authenticated user could exploit this to make MySQL crash, causing a denial of service. (CVE-2010-3837)
It was discovered that MySQL incorrectly handled certain queries using a mixed list of numeric and LONGBLOB arguments to the GREATEST() or LEAST() functions. An authenticated user could exploit this to make MySQL crash, causing a denial of service.
(CVE-2010-3838)
It was discovered that MySQL incorrectly handled queries with nested joins when used from stored procedures and prepared statements. An authenticated user could exploit this to make MySQL hang, causing a denial of service. This issue only affected Ubuntu 9.10, 10.04 LTS and 10.10. (CVE-2010-3839)
It was discovered that MySQL incorrectly handled improper WKB data passed to the PolyFromWKB() function. An authenticated user could exploit this to make MySQL crash, causing a denial of service.
(CVE-2010-3840)

See Also

http://www.ubuntu.com/usn/usn-1017-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

References

CVE	CVE-2010-2008
CVE	CVE-2010-3677
CVE	CVE-2010-3678
CVE	CVE-2010-3679
CVE	CVE-2010-3680
CVE	CVE-2010-3681
CVE	CVE-2010-3682
CVE	CVE-2010-3683
CVE	CVE-2010-3833
CVE	CVE-2010-3834
CVE	CVE-2010-3835
CVE	CVE-2010-3836
CVE	CVE-2010-3837
CVE	CVE-2010-3838
CVE	CVE-2010-3839
CVE	CVE-2010-3840
XREF	USN:1017-1

Ports

tcp/0

```
- Installed package : libmysqlclient16_5.1.37-1ubuntu5.1
  Fixed package     : libmysqlclient16_5.1.37-1ubuntu5.5

- Installed package : mysql-client-5.1_5.1.37-1ubuntu5.1
  Fixed package     : mysql-client-5.1_5.1.37-1ubuntu5.5

- Installed package : mysql-common_5.1.37-1ubuntu5.1
  Fixed package     : mysql-common_5.1.37-1ubuntu5.5

- Installed package : mysql-server-5.1_5.1.37-1ubuntu5.1
  Fixed package     : mysql-server-5.1_5.1.37-1ubuntu5.5

- Installed package : mysql-server-core-5.1_5.1.37-1ubuntu5.1
  Fixed package     : mysql-server-core-5.1_5.1.37-1ubuntu5.5
```

53220 - USN-1096-1 : subversion vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Philip Martin discovered that the Subversion mod_dav_svn module for Apache did not properly handle certain requests containing a lock token. A remote attacker could use this flaw to cause the service to crash, leading to a denial of service.

See Also

http://www.ubuntu.com/usn/usn-1096-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)

References

CVE	CVE-2011-0715
XREF	USN:1096-1

Ports

tcp/0

```
- Installed package : libapache2-svn_1.6.5dfsg-1ubuntu1
  Fixed package     : libapache2-svn_1.6.5dfsg-1ubuntu1.2

- Installed package : libsvn1_1.6.5dfsg-1ubuntu1
  Fixed package     : libsvn1_1.6.5dfsg-1ubuntu1.2

- Installed package : subversion_1.6.5dfsg-1ubuntu1
  Fixed package     : subversion_1.6.5dfsg-1ubuntu1.2
```

49102 - USN-982-1 : wget vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that Wget would use filenames provided by the server when following 3xx redirects. If a user or automated system were tricked into downloading a file from a malicious site, a remote attacker could create the file with an arbitrary name (e.g. .wgetrc), and possibly run arbitrary code.

See Also

http://www.ubuntu.com/usn/usn-982-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

References

CVE	CVE-2010-2252
XREF	OSVDB:66109
XREF	USN:982-1

Ports

tcp/0

```
- Installed package : wget_1.11.4-2ubuntu2
  Fixed package     : wget_1.11.4-2ubuntu2.1
```

51525 - USN-1042-2 : php5 regression

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

USN-1042-1 fixed vulnerabilities in PHP5. The fix for CVE-2010-3436 introduced a regression in the open_basedir restriction handling code. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
It was discovered that attackers might be able to bypass open_basedir() restrictions by passing a specially crafted filename.
(CVE-2010-3436)

See Also

http://www.ubuntu.com/usn/usn-1042-2/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

References

CVE	CVE-2010-3436
XREF	USN:1042-2

Ports

tcp/0

```
- Installed package : libapache2-mod-php5_5.2.10.dfsg.1-2ubuntu6.4
  Fixed package     : libapache2-mod-php5_5.2.10.dfsg.1-2ubuntu6.7

- Installed package : php5_5.2.10.dfsg.1-2ubuntu6.4
  Fixed package     : php5_5.2.10.dfsg.1-2ubuntu6.7

- Installed package : php5-common_5.2.10.dfsg.1-2ubuntu6.4
  Fixed package     : php5-common_5.2.10.dfsg.1-2ubuntu6.7

- Installed package : php5-mysql_5.2.10.dfsg.1-2ubuntu6.4
  Fixed package     : php5-mysql_5.2.10.dfsg.1-2ubuntu6.7
```

48282 - USN-965-1 : openldap, openldap2.2, openldap2.3 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Using the Codenomicon LDAPv3 test suite, Ilkka Mattila and Tuomas Salomäki discovered that the slap_modrdn2mods function in modrdn.c in OpenLDAP does not check the return value from a call to the smr_normalize function. A remote attacker could use specially crafted modrdn requests to crash the slapd daemon or possibly execute arbitrary code. (CVE-2010-0211)
Using the Codenomicon LDAPv3 test suite, Ilkka Mattila and Tuomas Salomäki discovered that OpenLDAP does not properly handle empty RDN strings. A remote attacker could use specially crafted modrdn requests to crash the slapd daemon. (CVE-2010-0212)
In the default installation under Ubuntu 8.04 LTS and later, attackers would be isolated by the OpenLDAP AppArmor profile for the slapd daemon.

See Also

http://www.ubuntu.com/usn/usn-965-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

References

CVE	CVE-2010-0211
CVE	CVE-2010-0212
XREF	OSVDB:66469
XREF	OSVDB:66470
XREF	USN:965-1

Ports

tcp/0

```
- Installed package : libldap-2.4-2_2.4.18-0ubuntu1
  Fixed package     : libldap-2.4-2_2.4.18-0ubuntu1.1
```

51846 - USN-1053-1 : subversion vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that Subversion incorrectly handled certain 'partial access' privileges in rare scenarios. Remote authenticated users could use this flaw to obtain sensitive information (revision properties). This issue only applied to Ubuntu 6.06 LTS.
(CVE-2007-2448)
It was discovered that the Subversion mod_dav_svn module for Apache did not properly handle a named repository as a rule scope. Remote authenticated users could use this flaw to bypass intended restrictions. This issue only applied to Ubuntu 9.10, 10.04 LTS, and 10.10. (CVE-2010-3315)
It was discovered that the Subversion mod_dav_svn module for Apache incorrectly handled the walk function. Remote authenticated users could use this flaw to cause the service to crash, leading to a denial of service. (CVE-2010-4539)
It was discovered that Subversion incorrectly handled certain memory operations. Remote authenticated users could use this flaw to consume large quantities of memory and cause the service to crash, leading to a denial of service. This issue only applied to Ubuntu 9.10, 10.04 LTS, and 10.10. (CVE-2010-4644)

See Also

http://www.ubuntu.com/usn/usn-1053-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

6.8 (CVSS2#AV:N/AC:L/Au:S/C:N/I:N/A:C)

References

CVE	CVE-2007-2448
CVE	CVE-2010-3315
CVE	CVE-2010-4539
CVE	CVE-2010-4644
XREF	USN:1053-1

Ports

tcp/0

```
- Installed package : libapache2-svn_1.6.5dfsg-1ubuntu1
```

```
  Fixed package     : libapache2-svn_1.6.5dfsg-1ubuntu1.1

- Installed package : libsvn1_1.6.5dfsg-1ubuntu1
  Fixed package     : libsvn1_1.6.5dfsg-1ubuntu1.1

- Installed package : subversion_1.6.5dfsg-1ubuntu1
  Fixed package     : subversion_1.6.5dfsg-1ubuntu1.1
```

51502 - USN-1042-1 : php5 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that an integer overflow in the XML UTF-8 decoding code could allow an attacker to bypass cross-site scripting (XSS) protections. This issue only affected Ubuntu 6.06 LTS, Ubuntu 8.04 LTS, and Ubuntu 9.10. (CVE-2009-5016)
It was discovered that the XML UTF-8 decoding code did not properly handle non-shortest form UTF-8 encoding and ill-formed subsequences in UTF-8 data, which could allow an attacker to bypass cross-site scripting (XSS) protections. (CVE-2010-3870)
It was discovered that attackers might be able to bypass open_basedir() restrictions by passing a specially crafted filename.
(CVE-2010-3436)
Maksymilian Arciemowicz discovered that a NULL pointer derefence in the ZIP archive handling code could allow an attacker to cause a denial of service through a specially crafted ZIP archive. This issue only affected Ubuntu 8.04 LTS, Ubuntu 9.10, Ubuntu 10.04 LTS, and Ubuntu 10.10. (CVE-2010-3709)
It was discovered that a stack consumption vulnerability in the filter_var() PHP function when in FILTER_VALIDATE_EMAIL mode, could allow a remote attacker to cause a denial of service. This issue only affected Ubuntu 8.04 LTS, Ubuntu 9.10, Ubuntu 10.04 LTS, and Ubuntu 10.10. (CVE-2010-3710)
It was discovered that the mb_strcut function in the Libmbfl library within PHP could allow an attacker to read arbitrary memory within the application process. This issue only affected Ubuntu 10.10.
(CVE-2010-4156)
Maksymilian Arciemowicz discovered that an integer overflow in the NumberFormatter::getSymbol function could allow an attacker to cause a denial of service. This issue only affected Ubuntu 10.04 LTS and Ubuntu 10.10.
(CVE-2010-4409)
Rick Regan discovered that when handing PHP textual representations of the largest subnormal double-precision floating-point number, the zend_strtod function could go into an infinite loop on 32bit x86 processors, allowing an attacker to cause a denial of service.
(CVE-2010-4645)

See Also

http://www.ubuntu.com/usn/usn-1042-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

References

CVE	CVE-2009-5016
CVE	CVE-2010-3436
CVE	CVE-2010-3709
CVE	CVE-2010-3710
CVE	CVE-2010-3870
CVE	CVE-2010-4156
CVE	CVE-2010-4409

CVE	CVE-2010-4645
XREF	USN:1042-1

Ports
tcp/0

```
- Installed package : libapache2-mod-php5_5.2.10.dfsg.1-2ubuntu6.4
  Fixed package     : libapache2-mod-php5_5.2.10.dfsg.1-2ubuntu6.6

- Installed package : php5_5.2.10.dfsg.1-2ubuntu6.4
  Fixed package     : php5_5.2.10.dfsg.1-2ubuntu6.6

- Installed package : php5-common_5.2.10.dfsg.1-2ubuntu6.4
  Fixed package     : php5-common_5.2.10.dfsg.1-2ubuntu6.6

- Installed package : php5-mysql_5.2.10.dfsg.1-2ubuntu6.4
  Fixed package     : php5-mysql_5.2.10.dfsg.1-2ubuntu6.6
```

51076 - USN-1029-1 : openssl vulnerabilities

Synopsis
The remote Ubuntu host is missing one or more security-related patches.

Description
It was discovered that an old bug workaround in the SSL/TLS server code allowed an attacker to modify the stored session cache ciphersuite. This could possibly allow an attacker to downgrade the ciphersuite to a weaker one on subsequent connections.
(CVE-2010-4180)
It was discovered that an old bug workaround in the SSL/TLS server code allowed allowed an attacker to modify the stored session cache ciphersuite. An attacker could possibly take advantage of this to force the use of a disabled cipher. This vulnerability only affects the versions of OpenSSL in Ubuntu 6.06 LTS, Ubuntu 8.04 LTS, and Ubuntu 9.10. (CVE-2008-7270)

See Also
http://www.ubuntu.com/usn/usn-1029-1/

Solution
Update the affected package(s).

Risk Factor
Medium

CVSS Base Score
4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

References
CVE	CVE-2008-7270
CVE	CVE-2010-4180
XREF	IAVA:2010-A-0167
XREF	USN:1029-1

Ports
tcp/0

```
- Installed package : libssl0.9.8_0.9.8g-16ubuntu3.1
  Fixed package     : libssl0.9.8_0.9.8g-16ubuntu3.5

- Installed package : openssl_0.9.8g-16ubuntu3.1
  Fixed package     : openssl_0.9.8g-16ubuntu3.5
```

50824 - USN-1022-1 : apr-util vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that APR-util did not properly handle memory when destroying APR buckets. An attacker could exploit this and cause a denial of service via memory exhaustion.

See Also

http://www.ubuntu.com/usn/usn-1022-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

References

CVE	CVE-2010-1623
XREF	USN:1022-1

Ports

tcp/0

```
- Installed package : libaprutil1_1.3.9+dfsg-1ubuntu1
  Fixed package     : libaprutil1_1.3.9+dfsg-1ubuntu1.1

- Installed package : libaprutil1-dbd-sqlite3_1.3.9+dfsg-1ubuntu1
  Fixed package     : libaprutil1-dbd-sqlite3_1.3.9+dfsg-1ubuntu1.1

- Installed package : libaprutil1-ldap_1.3.9+dfsg-1ubuntu1
  Fixed package     : libaprutil1-ldap_1.3.9+dfsg-1ubuntu1.1
```

49140 - USN-983-1 : sudo vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Markus Wuethrich discovered that sudo did not always verify the user when a group was specified in the Runas_Spec. A local attacker could exploit this to execute arbitrary code as root if sudo was configured to allow the attacker to use a program as a group when the attacker was not a part of that group.

See Also

http://www.ubuntu.com/usn/usn-983-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

6.2 (CVSS2#AV:L/AC:H/Au:N/C:C/I:C/A:C)

References

CVE	CVE-2010-2956
XREF	OSVDB:67842
XREF	USN:983-1

Ports

tcp/0

```
- Installed package : sudo_1.7.0-1ubuntu2.2
  Fixed package     : sudo_1.7.0-1ubuntu2.5
```

46855 - USN-950-1 : mysql-dfsg-5.0, mysql-dfsg-5.1 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that MySQL did not check privileges before uninstalling plugins. An authenticated user could uninstall arbitrary plugins, bypassing intended restrictions. This issue only affected Ubuntu 9.10 and 10.04 LTS. (CVE-2010-1621)
It was discovered that MySQL could be made to delete another user's data and index files. An authenticated user could use symlinks combined with the DROP TABLE command to possibly bypass privilege checks. (CVE-2010-1626)
It was discovered that MySQL incorrectly validated the table name argument of the COM_FIELD_LIST command. An authenticated user could use a specially- crafted table name to bypass privilege checks and possibly access other tables. (CVE-2010-1848)
Eric Day discovered that MySQL incorrectly handled certain network packets. A remote attacker could exploit this flaw and cause the server to consume all available resources, resulting in a denial of service. (CVE-2010-1849)
It was discovered that MySQL performed incorrect bounds checking on the table name argument of the COM_FIELD_LIST command. An authenticated user could use a specially-crafted table name to cause a denial of service or possibly execute arbitrary code. The default compiler options for affected releases should reduce the vulnerability to a denial of service. (CVE-2010-1850)

See Also

http://www.ubuntu.com/usn/usn-950-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

6.5 (CVSS2#AV:N/AC:L/Au:S/C:P/I:P/A:P)

References

CVE	CVE-2010-1621
CVE	CVE-2010-1626
CVE	CVE-2010-1848
CVE	CVE-2010-1849
CVE	CVE-2010-1850
XREF	USN:950-1

Exploitable with

CANVAS (true)

Ports

tcp/0

```
- Installed package : libmysqlclient16_5.1.37-1ubuntu5.1
  Fixed package     : libmysqlclient16_5.1.37-1ubuntu5.4

- Installed package : mysql-client-5.1_5.1.37-1ubuntu5.1
  Fixed package     : mysql-client-5.1_5.1.37-1ubuntu5.4

- Installed package : mysql-common_5.1.37-1ubuntu5.1
  Fixed package     : mysql-common_5.1.37-1ubuntu5.4

- Installed package : mysql-server-5.1_5.1.37-1ubuntu5.1
  Fixed package     : mysql-server-5.1_5.1.37-1ubuntu5.4
```

```
- Installed package : mysql-server-core-5.1_5.1.37-1ubuntu5.1
  Fixed package     : mysql-server-core-5.1_5.1.37-1ubuntu5.4
```

51584 - USN-1045-2 : util-linux update

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

USN-1045-1 fixed vulnerabilities in FUSE. This update to util-linux adds support for new options required by the FUSE update.
Original advisory details:
It was discovered that FUSE could be tricked into incorrectly updating the mtab file when mounting filesystems. A local attacker, with access to use FUSE, could unmount arbitrary locations, leading to a denial of service.

See Also

http://www.ubuntu.com/usn/usn-1045-2/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:P)

References

CVE	CVE-2010-3879
XREF	USN:1045-2

Ports

tcp/0

```
- Installed package : libblkid1_2.16-1ubuntu5
  Fixed package     : libblkid1_2.16-1ubuntu5.1

- Installed package : libuuid1_2.16-1ubuntu5
  Fixed package     : libuuid1_2.16-1ubuntu5.1

- Installed package : mount_2.16-1ubuntu5
  Fixed package     : mount_2.16-1ubuntu5.1

- Installed package : util-linux_2.16-1ubuntu5
  Fixed package     : util-linux_2.16-1ubuntu5.1

- Installed package : uuid-runtime_2.16-1ubuntu5
  Fixed package     : uuid-runtime_2.16-1ubuntu5.1
```

47679 - USN-959-1 : pam vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Denis Excoffier discovered that the PAM MOTD module in Ubuntu did not correctly handle path permissions when creating user file stamps. A local attacker could exploit this to gain root privilieges.

See Also

http://www.ubuntu.com/usn/usn-959-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

6.9 (CVSS2#AV:L/AC:M/Au:N/C:C/I:C/A:C)

References

CVE	CVE-2010-0832
XREF	OSVDB:66116
XREF	USN:959-1

Exploitable with

Core Impact (true)

Ports

tcp/0

```
- Installed package : libpam-modules_1.1.0-2ubuntu1
  Fixed package     : libpam-modules_1.1.0-2ubuntu1.1

- Installed package : libpam-runtime_1.1.0-2ubuntu1
  Fixed package     : libpam-runtime_1.1.0-2ubuntu1.1

- Installed package : libpam0g_1.1.0-2ubuntu1
  Fixed package     : libpam0g_1.1.0-2ubuntu1.1
```

55084 - USN-1124-1 : rsync vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that rsync incorrectly handled memory when certain recursion, deletion and ownership options were used. If a user were tricked into connecting to a malicious server, a remote attacker could cause a denial of service or execute arbitrary code with privileges of the user invoking the program.

See Also

http://www.ubuntu.com/usn/usn-1124-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

References

CVE	CVE-2011-1097
XREF	USN:1124-1

Ports

tcp/0

```
- Installed package : rsync_3.0.6-1ubuntu1
  Fixed package     : rsync_3.0.6-1ubuntu1.1
```

47575 - USN-956-1 : sudo vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Evan Broder and Anders Kaseorg discovered that sudo did not properly sanitize its environment when configured to use secure_path (the default in Ubuntu). A local attacker could exploit this to execute arbitrary code as root if sudo was configured to allow the attacker to use a program that interpreted the PATH environment variable.

See Also

http://www.ubuntu.com/usn/usn-956-1/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

6.2 (CVSS2#AV:L/AC:H/Au:N/C:C/I:C/A:C)

References

CVE	CVE-2010-1646
XREF	USN:956-1

Ports

tcp/0

```
- Installed package : sudo_1.7.0-1ubuntu2.2
  Fixed package     : sudo_1.7.0-1ubuntu2.4
```

49305 - USN-986-3 : dpkg vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

USN-986-1 fixed vulnerabilities in bzip2. dpkg statically links against libbz2 and needed to be rebuilt to use the updated libbz2.
Original advisory details:
An integer overflow was discovered in bzip2. If a user or automated system were tricked into decompressing a crafted bz2 file, an attacker could cause bzip2 or any application linked against libbz2 to crash or possibly execute code as the user running the program.

See Also

http://www.ubuntu.com/usn/usn-986-3/

Solution

Update the affected package(s).

Risk Factor

Medium

CVSS Base Score

5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

References

CVE	CVE-2010-0405
XREF	OSVDB:68167
XREF	USN:986-3

Ports

tcp/0

```
- Installed package : dpkg_1.15.4ubuntu2.1
  Fixed package     : dpkg_1.15.4ubuntu2.2

- Installed package : dpkg-dev_1.15.4ubuntu2.1
```

```
Fixed package     : dpkg-dev_1.15.4ubuntu2.2
```

51572 - USN-1044-1 : dbus vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Remi Denis-Courmont discovered that D-Bus did not properly validate the number of nested variants when validating D-Bus messages. A local attacker could exploit this to cause a denial of service.

See Also

http://www.ubuntu.com/usn/usn-1044-1/

Solution

Update the affected package(s).

Risk Factor

Low

CVSS Base Score

2.1 (CVSS2#AV:L/AC:L/Au:N/C:N/I:N/A:P)

References

CVE	CVE-2010-4352
XREF	USN:1044-1

Ports

tcp/0

```
- Installed package : libdbus-1-3_1.2.16-0ubuntu9
  Fixed package     : libdbus-1-3_1.2.16-0ubuntu9.1
```

52479 - USN-1077-1 : fuse vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that FUSE would incorrectly follow symlinks when checking mountpoints under certain conditions. A local attacker, with access to use FUSE, could unmount arbitrary locations, leading to a denial of service.

See Also

http://www.ubuntu.com/usn/usn-1077-1/

Solution

Update the affected package(s).

Risk Factor

Low

CVSS Base Score

3.3 (CVSS2#AV:L/AC:M/Au:N/C:N/I:P/A:P)

References

CVE	CVE-2010-0789
CVE	CVE-2011-0541
CVE	CVE-2011-0542
CVE	CVE-2011-0543
XREF	USN:1077-1

XREF CWE:59

Ports
tcp/0

```
  - Installed package : fuse-utils_2.7.4-1.1ubuntu4.3
    Fixed package     : fuse-utils_2.7.4-1.1ubuntu4.5

  - Installed package : libfuse2_2.7.4-1.1ubuntu4.3
    Fixed package     : libfuse2_2.7.4-1.1ubuntu4.5
```

33851 - Network daemons not managed by the package system

Synopsis

Some daemon processes on the remote host are associated with programs that have been installed manually.

Description

Some daemon processes on the remote host are associated with programs that have been installed manually.
System administration best practice dictates that an operating system's native package management tools be used to manage software installation, updates, and removal whenever possible.

Solution

Use packages supplied by the operating system vendor whenever possible.
And make sure that manual software installation agrees with your organization's acceptable use and security policies.

Risk Factor

Low

CVSS Base Score

2.1 (CVSS2#AV:N/AC:H/Au:S/C:N/I:P/A:N)

Ports
tcp/0

```
The following running daemons are not managed by dpkg :

/usr/local/proftpd/sbin/proftpd
/usr/local/subversion/bin/svnserve
```

18261 - Apache Banner Linux Distribution Disclosure

Synopsis

The name of the Linux distribution running on the remote host was found in the banner of the web server.

Description

This script extracts the banner of the Apache web server and attempts to determine which Linux distribution the remote host is running.

Solution

If you do not wish to display this information, edit httpd.conf and set the directive 'ServerTokens Prod' and restart Apache.

Risk Factor

None

Ports
tcp/0

```
The linux distribution detected was :
 - Ubuntu 9.10 (karmic)
```

12634 - Authenticated Check: OS Name and Installed Package Enumeration

Synopsis

This plugin gathers information about the remote host via an authenticated session.

Description

This plugin logs into the remote host using SSH, RSH, RLOGIN, Telnet or local commands and extracts the list of installed packages.

If using SSH, the scan should be configured with a valid SSH public key and possibly an SSH passphrase (if the SSH public key is protected by a passphrase).

Solution

n/a

Risk Factor

None

Ports

tcp/0

```
It was possible to log into the remote host using the supplied password
The output of "uname -a" is :
Linux SECURITYFAIL 2.6.31-23-generic-pae #75-Ubuntu SMP Fri Mar 18 19:14:10 UTC 2011 i686 GNU/
Linux

The remote Debian system is :
squeeze/sid

This is a Ubuntu system

Local security checks have been enabled for this host.
```

34098 - BIOS version (SSH)

Synopsis

The BIOS version could be read.

Description

Using the SMBIOS (aka DMI) interface, it was possible to get the BIOS vendor and version.

Solution

N/A

Risk Factor

None

Ports

tcp/0

```
Version      : 6.00
Vendor       : Phoenix Technologies LTD
Release Date : 06/02/2011
```

45433 - Memory Information (via DMI)

Synopsis

Information about the remote system's memory devices can be read.

Description

Using the SMBIOS (aka DMI) interface, it was possible to retrieve information about the remote system's memory devices, such as the total amount of installed memory.

Solution

n/a

Risk Factor

None

Ports

tcp/0

```
Total memory : 512 MB
```

35351 - System Information Enumeration (via DMI)

Synopsis

Information about the remote system's hardware can be read.

Description

Using the SMBIOS (aka DMI) interface, it was possible to retrieve information about the remote system's hardware, such as its product name and serial number.

Solution

n/a

Risk Factor

None

Ports

tcp/0

```
Serial Number : VMware-56 4d 62 00 d6 4a 6d be-84 0f 5b 8b fd 16 e8 6c
Product Name  : VMware Virtual Platform
```

45432 - Processor Information (via DMI)

Synopsis

Information about the remote system's processor can be read.

Description

Using the SMBIOS (aka DMI) interface, it was possible to retrieve information about the remote system's hardware, such as its processor type.

Solution

n/a

Risk Factor

None

Ports

tcp/0

```
Nessus detected 1 processor :

Current Speed   : 2200 MHz
Version         : Pentium(R) Pro
Manufacturer    : GenuineIntel
External Clock  : Unknown
Family          : Pentium Pro
Type            : Central Processor
```

56468 - Time of Last System Startup

Synopsis

The system has been started.

Description

Using the supplied credentials, Nessus was able to determine when the host was last started.

Solution

n/a

Risk Factor

None

Ports

tcp/0

```
reboot   system boot  2.6.31-23-generi Fri Feb 24 11:11 - 18:30  (07:18)
reboot   system boot  2.6.31-23-generi Fri Feb 24 11:10 - 11:11  (00:01)
reboot   system boot  2.6.31-23-generi Fri Feb 24 09:31 - 11:10  (01:38)
reboot   system boot  2.6.31-21-generi Tue Feb 21 15:02 - 09:31 (2+18:28)
reboot   system boot  2.6.31-21-generi Tue Feb 21 14:18 - 15:02  (00:43)
reboot   system boot  2.6.31-21-generi Wed Feb 15 10:55 - 14:18 (6+03:23)

wtmp begins Wed Feb 15 10:55:00 2012
```

33276 - Enumerate MAC Addresses via SSH

Synopsis

This plugin enumerates MAC addresses on a remote host.

Description

By connecting to the remote host via SSH with the supplied credentials, this plugin enumerates MAC addresses.

Solution

Disable any unused interfaces.

Risk Factor

None

Ports

tcp/0

```
The following MAC address exists on the remote host :

  - 00:0c:29:16:e8:6c (interface eth0)
```

25203 - Enumerate IPv4 Interfaces via SSH

Synopsis

This plugin enumerates IPv4 interfaces on a remote host.

Description

By connecting to the remote host via SSH with the supplied credentials, this plugin enumerates network interfaces configured with IPv4 addresses.

Solution

Disable any unused IPv4 interfaces.

Risk Factor

None

Ports

tcp/0

```
The following IPv4 addresses are set on the remote host :

 - 192.168.150.131 (on interface eth0)
 - 127.0.0.1 (on interface lo)
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host seems to be a VMware virtual machine.

Description

According to the MAC address of its network adapter, the remote host is a VMware virtual machine.
Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Solution

n/a

Risk Factor

None

Ports

tcp/0

25202 - Enumerate IPv6 Interfaces via SSH

Synopsis

This plugin enumerates IPv6 interfaces on a remote host.

Description

By connecting to the remote host via SSH with the supplied credentials, this plugin enumerates network interfaces configured with IPv6 addresses.

Solution

Disable IPv6 if you do not actually using it. Otherwise, disable any unused IPv6 interfaces.

Risk Factor

None

Ports

tcp/0

```
The following IPv6 interfaces are set on the remote host :

 - fe80::20c:29ff:fea1:2203 (on interface eth0)
 - fe80::20c:29ff:fe16:e86c (on interface eth0)
 - ::1 (on interface lo)
```

55472 - Device Hostname

Synopsis

It is possible to determine the remote system hostname.

Description

This plugin reports a device's hostname collected via SSH or WMI.

Solution

n/a

Risk Factor

None

Ports

tcp/0

```
  Hostname : SECURITYFAIL
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes, (TCP/IP, SMB, HTTP, NTP, SNMP, etc...) it is possible to guess the name of the remote operating system in use, and sometimes its version.

Solution

n/a

Risk Factor

None

Ports

tcp/0

```
Remote operating system : Linux Kernel 2.6.31-23-generic-pae on Ubuntu 9.10
Confidence Level : 100
Method : LinuxDistribution


The remote host is running Linux Kernel 2.6.31-23-generic-pae on Ubuntu 9.10
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It is possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.
Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

Solution

n/a

Risk Factor

None

Ports

tcp/0

```
The remote operating system matched the following CPE :

  cpe:/o:canonical:ubuntu_linux:9.10 -> Canonical Ubuntu Linux 9.10

Following application CPE's matched on the remote system :

  cpe:/a:openbsd:openssh:5.1
  cpe:/a:apache:http_server:2.2.12 -> Apache Software Foundation Apache HTTP Server 2.2.12
```

7/tcp

14272 - netstat portscanner (SSH)

Synopsis

Remote open ports are enumerated via SSH.

Description

This plugin runs 'netstat' (or an equivalent command) on the remote machine to enumerate open ports.
See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Ports

tcp/7

```
Port 7/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Ports

tcp/7

```
An echo server is running on this port.
```

25221 - Remote listeners enumeration

Synopsis

Using netstat, it is possible to identify daemons listening on the remote port.

Description

By logging into the remote host and using the Linux-specific 'netstat
-anp' command, it was possible to obtain the name of the processe listening on the remote port.

Solution

n/a

Risk Factor

None

Ports

tcp/7

```
The Linux process '/usr/sbin/xinetd' is listening on this port.
```

7/udp

14272 - netstat portscanner (SSH)

Synopsis

Remote open ports are enumerated via SSH.

Description

This plugin runs 'netstat' (or an equivalent command) on the remote machine to enumerate open ports.
See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Ports

udp/7

```
Port 7/udp was found to be open
```

25221 - Remote listeners enumeration

Synopsis

Using netstat, it is possible to identify daemons listening on the remote port.

Description

By logging into the remote host and using the Linux-specific 'netstat
-anp' command, it was possible to obtain the name of the processe listening on the remote port.

Solution

n/a

Risk Factor

None

Ports

udp/7

```
The Linux process '/usr/sbin/xinetd' is listening on this port.
```

9/tcp

14272 - netstat portscanner (SSH)

Synopsis

Remote open ports are enumerated via SSH.

Description

This plugin runs 'netstat' (or an equivalent command) on the remote machine to enumerate open ports.
See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Ports

tcp/9

```
Port 9/tcp was found to be open
```

25221 - Remote listeners enumeration

Synopsis

Using netstat, it is possible to identify daemons listening on the remote port.

Description

By logging into the remote host and using the Linux-specific 'netstat
-anp' command, it was possible to obtain the name of the processe listening on the remote port.

Solution

n/a

Risk Factor

None

Ports

tcp/9

```
The Linux process '/usr/sbin/xinetd' is listening on this port.
```

9/udp

14272 - netstat portscanner (SSH)

Synopsis

Remote open ports are enumerated via SSH.

Description

This plugin runs 'netstat' (or an equivalent command) on the remote machine to enumerate open ports.
See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Ports

udp/9

```
Port 9/udp was found to be open
```

25221 - Remote listeners enumeration

Synopsis

Using netstat, it is possible to identify daemons listening on the remote port.

Description

By logging into the remote host and using the Linux-specific 'netstat
-anp' command, it was possible to obtain the name of the processe listening on the remote port.

Solution

n/a

Risk Factor

None

Ports

udp/9

```
The Linux process '/usr/sbin/xinetd' is listening on this port.
```

13/tcp

14272 - netstat portscanner (SSH)

Synopsis

Remote open ports are enumerated via SSH.

Description

This plugin runs 'netstat' (or an equivalent command) on the remote machine to enumerate open ports.
See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Ports

tcp/13

```
Port 13/tcp was found to be open
```

11153 - Service Detection (HELP Request)

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a 'HELP' request.

Solution

n/a

Risk Factor

None

Ports

tcp/13

```
Daytime is running on this port.
```

25221 - Remote listeners enumeration

Synopsis

Using netstat, it is possible to identify daemons listening on the remote port.

Description

By logging into the remote host and using the Linux-specific 'netstat
-anp' command, it was possible to obtain the name of the processe listening on the remote port.

Solution

n/a

Risk Factor

None

Ports

tcp/13

```
The Linux process '/usr/sbin/xinetd' is listening on this port.
```

13/udp

14272 - netstat portscanner (SSH)

Synopsis

Remote open ports are enumerated via SSH.

Description

This plugin runs 'netstat' (or an equivalent command) on the remote machine to enumerate open ports.
See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Ports

udp/13

```
Port 13/udp was found to be open
```

25221 - Remote listeners enumeration

Synopsis

Using netstat, it is possible to identify daemons listening on the remote port.

Description

By logging into the remote host and using the Linux-specific 'netstat
-anp' command, it was possible to obtain the name of the processe listening on the remote port.

Solution

n/a

Risk Factor

None

Ports

udp/13

```
The Linux process '/usr/sbin/xinetd' is listening on this port.
```

19/tcp

14272 - netstat portscanner (SSH)

Synopsis

Remote open ports are enumerated via SSH.

Description

This plugin runs 'netstat' (or an equivalent command) on the remote machine to enumerate open ports.
See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Ports

tcp/19

```
Port 19/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Ports

tcp/19

```
A chargen server is running on this port.
```

25221 - Remote listeners enumeration

Synopsis

Using netstat, it is possible to identify daemons listening on the remote port.

Description

By logging into the remote host and using the Linux-specific 'netstat
-anp' command, it was possible to obtain the name of the processe listening on the remote port.

Solution

n/a

Risk Factor

None

Ports

tcp/19

```
The Linux process '/usr/sbin/xinetd' is listening on this port.
```

19/udp

14272 - netstat portscanner (SSH)

Synopsis

Remote open ports are enumerated via SSH.

Description

This plugin runs 'netstat' (or an equivalent command) on the remote machine to enumerate open ports.
See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Ports

udp/19

```
Port 19/udp was found to be open
```

25221 - Remote listeners enumeration

Synopsis

Using netstat, it is possible to identify daemons listening on the remote port.

Description

By logging into the remote host and using the Linux-specific 'netstat
-anp' command, it was possible to obtain the name of the processe listening on the remote port.

Solution

n/a

Risk Factor

None

Ports

udp/19

```
The Linux process '/usr/sbin/xinetd' is listening on this port.
```

21/tcp

14272 - netstat portscanner (SSH)

Synopsis

Remote open ports are enumerated via SSH.

Description

This plugin runs 'netstat' (or an equivalent command) on the remote machine to enumerate open ports.
See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Ports

tcp/21

```
Port 21/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Ports

tcp/21

```
An FTP server is running on this port.
```

10092 - FTP Server Detection

Synopsis

An FTP server is listening on this port.

Description

It is possible to obtain the banner of the remote FTP server by connecting to the remote port.

Solution

N/A

Risk Factor

None

Ports

tcp/21

```
The remote FTP banner is :

220 ProFTPD 1.2.5 Server (ProFTPD Default Installation) [SECURITYFAIL.localdomain]
```

25221 - Remote listeners enumeration

Synopsis

Using netstat, it is possible to identify daemons listening on the remote port.

Description

By logging into the remote host and using the Linux-specific 'netstat
-anp' command, it was possible to obtain the name of the processe listening on the remote port.

Solution

n/a

Risk Factor

None

Ports

tcp/21

```
The Linux process '/usr/local/proftpd/sbin/proftpd' is listening on this port.
```

22/tcp

14272 - netstat portscanner (SSH)

Synopsis

Remote open ports are enumerated via SSH.

Description

This plugin runs 'netstat' (or an equivalent command) on the remote machine to enumerate open ports.
See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Ports

tcp/22

```
Port 22/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Ports

tcp/22

```
An SSH server is running on this port.
```

10267 - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution

n/a

Risk Factor

None

Ports

tcp/22

```
SSH version : SSH-2.0-OpenSSH_5.1p1 Debian-6ubuntu2
SSH supported authentication : publickey,password
```

25221 - Remote listeners enumeration

Synopsis

Using netstat, it is possible to identify daemons listening on the remote port.

Description

By logging into the remote host and using the Linux-specific 'netstat
-anp' command, it was possible to obtain the name of the processe listening on the remote port.

Solution

n/a

Risk Factor

None

Ports

tcp/22

```
The Linux process '/usr/sbin/sshd' is listening on this port.
```

23/tcp

14272 - netstat portscanner (SSH)

Synopsis

Remote open ports are enumerated via SSH.

Description

This plugin runs 'netstat' (or an equivalent command) on the remote machine to enumerate open ports.
See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Ports

tcp/23

```
Port 23/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Ports

tcp/23

```
A telnet server is running on this port.
```

10281 - Telnet Server Detection

Synopsis

A Telnet server is listening on the remote port.

Description

The remote host is running a Telnet server, a remote terminal server.

Solution

Disable this service if you do not use it.

Risk Factor

None

Ports

tcp/23

```
Here is the banner from the remote Telnet server :

------------------------------ snip ------------------------------
Ubuntu 9.10
SECURITYFAIL login:
------------------------------ snip ------------------------------
```

25221 - Remote listeners enumeration

Synopsis

Using netstat, it is possible to identify daemons listening on the remote port.

Description

By logging into the remote host and using the Linux-specific 'netstat
-anp' command, it was possible to obtain the name of the processe listening on the remote port.

Solution

n/a

Risk Factor

None

Ports

tcp/23

```
The Linux process '/usr/sbin/xinetd' is listening on this port.
```

25/tcp

14272 - netstat portscanner (SSH)

Synopsis

Remote open ports are enumerated via SSH.

Description

This plugin runs 'netstat' (or an equivalent command) on the remote machine to enumerate open ports.
See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Ports

tcp/25

```
Port 25/tcp was found to be open
```

25221 - Remote listeners enumeration

Synopsis

Using netstat, it is possible to identify daemons listening on the remote port.

Description

By logging into the remote host and using the Linux-specific 'netstat
-anp' command, it was possible to obtain the name of the processe listening on the remote port.

Solution

n/a

Risk Factor

None

Ports

tcp/25

```
The Linux process '/usr/lib/postfix/master' is listening on this port.
```

37/tcp

14272 - netstat portscanner (SSH)

Synopsis

Remote open ports are enumerated via SSH.

Description

This plugin runs 'netstat' (or an equivalent command) on the remote machine to enumerate open ports.
See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Ports

tcp/37

```
Port 37/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Ports

tcp/37

```
A time server is running on this port.
```

25221 - Remote listeners enumeration

Synopsis

Using netstat, it is possible to identify daemons listening on the remote port.

Description

By logging into the remote host and using the Linux-specific 'netstat
-anp' command, it was possible to obtain the name of the processe listening on the remote port.

Solution

n/a

Risk Factor

None

Ports

tcp/37

```
The Linux process '/usr/sbin/xinetd' is listening on this port.
```

37/udp

14272 - netstat portscanner (SSH)

Synopsis

Remote open ports are enumerated via SSH.

Description

This plugin runs 'netstat' (or an equivalent command) on the remote machine to enumerate open ports.
See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Ports

udp/37

```
Port 37/udp was found to be open
```

25221 - Remote listeners enumeration

Synopsis

Using netstat, it is possible to identify daemons listening on the remote port.

Description

By logging into the remote host and using the Linux-specific 'netstat
-anp' command, it was possible to obtain the name of the processe listening on the remote port.

Solution

n/a

Risk Factor

None

Ports

udp/37

```
The Linux process '/usr/sbin/xinetd' is listening on this port.
```

80/tcp

14272 - netstat portscanner (SSH)

Synopsis

Remote open ports are enumerated via SSH.

Description

This plugin runs 'netstat' (or an equivalent command) on the remote machine to enumerate open ports.
See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Ports

tcp/80

```
Port 80/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Ports

tcp/80

```
A web server is running on this port.
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

Ports

tcp/80

```
The remote web server type is :

Apache/2.2.12 (Ubuntu)

You can set the directive 'ServerTokens Prod' to limit the information
emanating from the server in its response headers.
```

25221 - Remote listeners enumeration

Synopsis

Using netstat, it is possible to identify daemons listening on the remote port.

Description

By logging into the remote host and using the Linux-specific 'netstat
-anp' command, it was possible to obtain the name of the processe listening on the remote port.

Solution

n/a

Risk Factor

None

Ports

tcp/80

```
The Linux process '/usr/lib/apache2/mpm-prefork/apache2' is listening on this port.
```

3306/tcp

14272 - netstat portscanner (SSH)

Synopsis

Remote open ports are enumerated via SSH.

Description

This plugin runs 'netstat' (or an equivalent command) on the remote machine to enumerate open ports.
See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Ports

tcp/3306

```
Port 3306/tcp was found to be open
```

11153 - Service Detection (HELP Request)

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a 'HELP' request.

Solution

n/a

Risk Factor

None

Ports

tcp/3306

```
A MySQL server is running on this port.
```

10719 - MySQL Server Detection

Synopsis

A database server is listening on the remote port.

Description

The remote host is running MySQL, an open-source database server.

Solution

n/a

Risk Factor

None

Ports

tcp/3306

```
Version  : 5.1.37-1ubuntu5.1
Protocol : 10
Server Status : SERVER_STATUS_AUTOCOMMIT
Server Capabilities :
  CLIENT_LONG_PASSWORD (new more secure passwords)
  CLIENT_FOUND_ROWS (Found instead of affected rows)
  CLIENT_LONG_FLAG (Get all column flags)
  CLIENT_CONNECT_WITH_DB (One can specify db on connect)
  CLIENT_NO_SCHEMA (Don't allow database.table.column)
  CLIENT_COMPRESS (Can use compression protocol)
  CLIENT_ODBC (ODBC client)
  CLIENT_LOCAL_FILES (Can use LOAD DATA LOCAL)
  CLIENT_IGNORE_SPACE (Ignore spaces before "("
  CLIENT_PROTOCOL_41 (New 4.1 protocol)
  CLIENT_INTERACTIVE (This is an interactive client)
  CLIENT_SIGPIPE (IGNORE sigpipes)
  CLIENT_TRANSACTIONS (Client knows about transactions)
  CLIENT_RESERVED (Old flag for 4.1 protocol)
  CLIENT_SECURE_CONNECTION (New 4.1 authentication)
```

25221 - Remote listeners enumeration

Synopsis

Using netstat, it is possible to identify daemons listening on the remote port.

Description

By logging into the remote host and using the Linux-specific 'netstat
-anp' command, it was possible to obtain the name of the processe listening on the remote port.

Solution

n/a

Risk Factor

None

Ports

tcp/3306

```
The Linux process '/usr/sbin/mysqld' is listening on this port.
```

3690/tcp

14272 - netstat portscanner (SSH)

Synopsis

Remote open ports are enumerated via SSH.

Description

This plugin runs 'netstat' (or an equivalent command) on the remote machine to enumerate open ports.
See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Ports

tcp/3690

```
Port 3690/tcp was found to be open
```

11153 - Service Detection (HELP Request)

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a 'HELP' request.

Solution

n/a

Risk Factor

None

Ports

tcp/3690

```
A SubVersion server is running on this port.
```

25221 - Remote listeners enumeration

Synopsis

Using netstat, it is possible to identify daemons listening on the remote port.

Description

By logging into the remote host and using the Linux-specific 'netstat
-anp' command, it was possible to obtain the name of the processe listening on the remote port.

Solution

n/a

Risk Factor

None

Ports

tcp/3690

```
The Linux process '/usr/local/subversion/bin/svnserve' is listening on this port.
```