Nessus Report

Report

21/Mar/2012:16:43:56 GMT

Table Of Contents

Vulnerabilities By Plugin

33929 (4) - PCI DSS compliance

Synopsis

Nessus has determined that this host is NOT COMPLIANT with the PCI DSS requirements.

Description

The remote web server is vulnerable to cross-site scripting (XSS) attacks, implements old SSL2.0 cryptography, runs obsolete software, or is affected by dangerous vulnerabilities (CVSS base score >= 4).

See Also

http://www.pcisecuritystandards.org/

http://en.wikipedia.org/wiki/PCI_DSS

Risk Factor

None

Hosts

192.168.150.100 (tcp/0)

```
+ The remote operating system is not maintained any more. See :
   http://www.nessus.org/plugins/index.php?view=single&id=47709
+ Unsupported software was found. See :
   http://www.nessus.org/plugins/index.php?view=single&id=34460
+ A web server is vulnerable to cross-site scripting (XSS)
+ 21 high risk flaws were found. See :
   http://www.nessus.org/plugins/index.php?view=single&id=34477
   http://www.nessus.org/plugins/index.php?view=single&id=21193
   http://www.nessus.org/plugins/index.php?view=single&id=12209
   http://www.nessus.org/plugins/index.php?view=single&id=22194
   http://www.nessus.org/plugins/index.php?view=single&id=35362
   http://www.nessus.org/plugins/index.php?view=single&id=21334
   http://www.nessus.org/plugins/index.php?view=single&id=19407
   http://www.nessus.org/plugins/index.php?view=single&id=11835
   http://www.nessus.org/plugins/index.php?view=single&id=19408
   http://www.nessus.org/plugins/index.php?view=single&id=20008
   http://www.nessus.org/plugins/index.php?view=single& [...]
```

192.168.150.100 (tcp/80)

```
The remote web server is vulnerable to cross-site scripting (XSS)
```

192.168.150.131 (tcp/0)

```
+ Directory browsing is enabled on some web servers
  http://192.168.150.131/phpmyadmin/themes/darkblue_orange/img/
  http://192.168.150.131/phpmyadmin/themes/darkblue_orange/css/
  http://192.168.150.131/dvwa/dvwa/includes/DBMS/
  http://192.168.150.131/phpmyadmin/themes/darkblue_orange/
  http://192.168.150.131/awstatsicons/os/
  http://192.168.150.131/dvwa/dvwa/css/
  http://192.168.150.131/phpmyadmin/themes/original/css/
  http://192.168.150.131/phpmyadmin/themes/
  http://192.168.150.131/awstatsicons/
  http://192.168.150.131/dvwa/dvwa/
  http://192.168.150.131/phpmyadmin/themes/original/
  http://192.168.150.131/board/images/
  http://192.168.150.131/phpmyadmin/themes/original/img/
  http://192.168.150.131/dvwa/dvwa/images/
  http://192.168.150.131/awstatsicons/other/
  http://192.168.150.131/awstatsicons/clock/
  http://192.168.150.131/dvwa/dvwa/includes/
  http://192.168.150.131/dvwa/dvwa/js/
  http://192.168.150.131/awstatsicons/browser/
  http://192.168.150.131/awstatsicons/cpu/
  http://192.168.150. [...]
```

192.168.150.131 (tcp/80)

```
The remote web server is vulnerable to cross-site scripting (XSS)
```

56208 (5) - PCI DSS compliance : Insecure Communication Has Been Detected

Synopsis

An insecure port, protocol or service has been detected.

Description

Applications that fail to adequately encrypt network traffic using strong cryptography are at increased risk of being compromised and exposing cardholder data. If an attacker is able to exploit weak cryptographic processes, he/she may be able to gain control of an application or even gain clear-text access to encrypted data.

Solution

Properly encrypt all authenticated and sensitive communications.

Risk Factor

Medium

Hosts

192.168.150.100 (tcp/21)

```
This FTP server does not support 'AUTH TLS'.
```

192.168.150.131 (tcp/21)

```
This FTP server does not support 'AUTH TLS'.
```

192.168.150.131 (tcp/23)

```
Nessus collected the following banner from the remote Telnet server :

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

192.168.150.131 (tcp/80)

```
Page : /board/
Destination page : /board/index.php
Input name : password


Page : /board/?D=A
Destination page : /board/index.php
Input name : password


Page : /phpmyadmin/
Destination page : index.php
Input name : pma_password


Page : /phpmyadmin/?D=A
Destination page : index.php
Input name : pma_password


Page : /board/register.php
Destination page : register_script.php
Input name : password
Input name : password2


Page : /board/index.php?username=&password=&cookie=yes&submit=Submit&page=&forumid=
Destination page : /board/index.php
Input name : password


Page : /board/message.php?reply=0
Destination page : /board/message.php
Input name : password
```

```
Page : /dvwa/login.php
Destination page : login.php
Input name : password


Page : /phpmyadmin/index.php?
phpMyAdmin=ec1a515150b712760566bab7a00e0a4bf149235b&db=&table=&lang=en-
utf-8&convcharset=utf-8&collation_connection=utf8_general_ci&token=5464357048baf63cc6907e2b30f403e7&phpMyAdmin
utf-8&phpMyAdmin=ec1a [...]
```

33931 (1) - PCI DSS Compliance: Tests Requirements

Synopsis

Nessus is not properly configured for PCI DSS validation.

Description

The scan settings did not fulfill the PCI DSS scan validation requirements. Even if the technical tests passed, this report may be insufficient to certify this server.

See Also

http://en.wikipedia.org/wiki/PCI_DSS

http://www.nessus.org/u?870f3331

Risk Factor

None

Hosts

192.168.150.131 (tcp/0)

```
+ A database is  reachable on a private network.
  Start the scan again from a public IP address to check that it is
  not reachable from the Internet.
```

56306 (1) - Web Server Allows Password Auto-Completion (PCI-DSS variant)

Synopsis

Auto-complete is not disabled on password fields.

Description

The remote web server contains at least HTML form field containing an input of type 'password' where 'autocomplete' is not set to 'off'.
While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or their machine is compromised at some point.

Solution

Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.

Risk Factor

Medium

CVSS Base Score

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

Hosts

192.168.150.131 (tcp/80)

```
Page : /board/
Destination Page : /board/index.php
Input name : password



Page : /board/?D=A
Destination Page : /board/index.php
Input name : password



Page : /phpmyadmin/
Destination Page : index.php
Input name : pma_password



Page : /phpmyadmin/?D=A
Destination Page : index.php
Input name : pma_password



Page : /board/register.php
Destination Page : register_script.php
Input name : password
Input name : password2



Page : /board/index.php?username=&password=&cookie=yes&submit=Submit&pag
e=&forumid=
Destination Page : /board/index.php
Input name : password



Page : /board/message.php?reply=0
Destination Page : /board/message.php
Input name : password
```

```
Page : /phpmyadmin/index.php?phpMyAdmin=ec1a515150b712760566bab7a00e0a4b
f149235b&db=&table=&lang=en-utf-8&convcharset=utf-8&collation_connection
=utf8_general_ci&token=5464357048baf63cc6907e2b30f403e7&phpMyAdmin=ec1a5
15150b712760566bab7a00e0a4bf149235b&lang=srlat-utf-8&phpMyAdmin=ec1a5151
50b712760566bab7a00e0a4bf149235b
Destination Page : i [...]
```

56209 (2) - PCI DSS compliance : Remote Access Software Has Been Detected

Synopsis

A remote access software has been detected.

Description

Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely per Appendix C in the ASV Program Guide, or disabled / removed. Please consult your ASV if you have questions about this Special Note.

Solution

n/a

Risk Factor

None

Hosts

192.168.150.100 (tcp/0)

```
An SMB server is running on the remote host.

A CIFS server is running on the remote host.
```

192.168.150.131 (tcp/0)

```
An SSH server (remote terminal) is running on the remote host.

A Telnet server (remote terminal) is running on the remote host.
```