TENABLE NETWORK SECURITY

# RDP Service Vulnerabilities

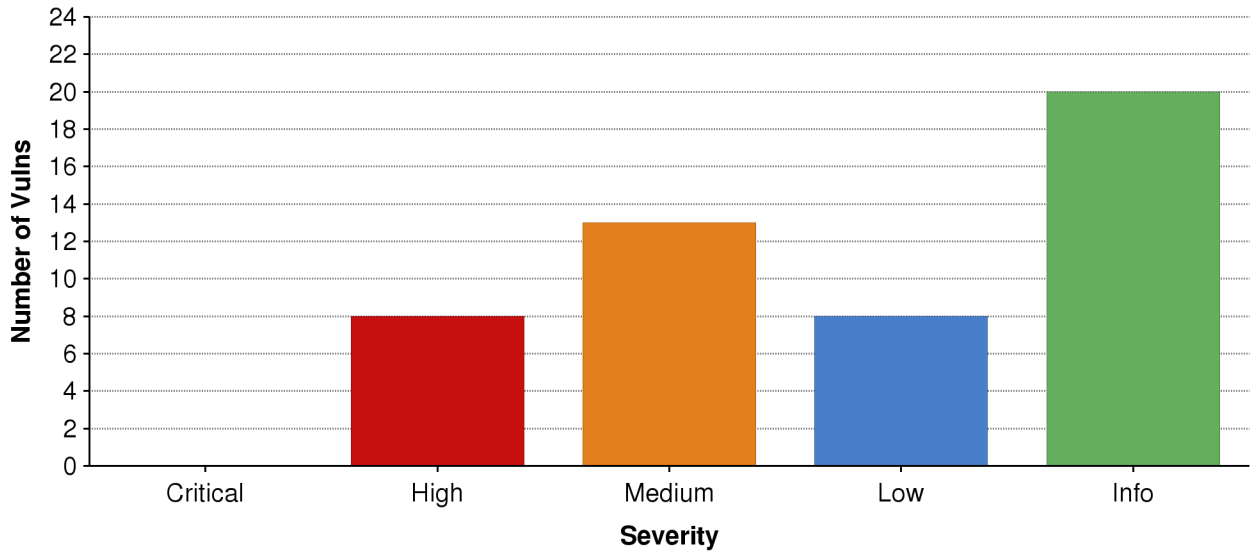
## April 11, 2012 at 8:55pm CDT
## [dbreslin]



TENABLE
Network Security®

# RDP Vulnerability Summary

## RDP Vulnerability Summary



# RDP Miscellaneous

### Service Count

| Total |
|---|
| 10 |

### Not FIPS-140 Compliant

| Total |
|---|
| 8 |

### MS12-020 Uncredentialed Check

| Total |
|---|
| 8 |

### Vulnerable to MiTM Attack

| Total |
|---|
| 8 |

# RDP Vulnerability Details - Info Severity Excluded

**RDP Vulnerability Details - Info Severity Excluded**

| Plugin | Plugin Name | Severity | Family |
|---|---|---|---|
| 58435 | MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) | High | Windows |
| An arbitrary remote code vulnerability exists in the implementation / of the Remote Desktop Protocol (RDP) on the remote Windows host. The / vulnerability is due to the way that RDP accesses an object in memory / that has been improperly initialized or has been deleted. / / If RDP has been enabled on the affected system, an unauthenticated, / remote attacker could leverage this vulnerability to cause the system / to execute arbitrary code by sending a sequence of specially crafted / RDP packets to it. / / This plugin also checks for a denial of service vulnerability in / Microsoft Terminal Server. / / Note that this script does not detect the vulnerability if the / 'Allow connections only from computers running Remote Desktop with / Network Level Authentication' setting is enabled or the security / layer is set to 'SSL (TLS 1.0)' on the remote host. | | | |
| **Hosts in Repository 'nocredentials':**<br><br>192.168.10.3 - MAC: 08:00:27:f8:ba:1f DNS: dt0100.itsdept.com NetBIOS: ITSDEPT\DT0100<br>192.168.10.15 - MAC: 08:00:27:f8:ba:2e DNS: dt0109.itsdept.com NetBIOS: ITSDEPT\DT0109<br>192.168.10.23 - MAC: 08:00:27:1e:10:00 DNS: dt0130.itsdept.com NetBIOS: ITSDEPT\DT0130<br>192.168.10.88 - MAC: 08:00:27:09:01:ba DNS: dt0147.itsdept.com NetBIOS: ITSDEPT\DT0147<br>192.168.20.2 - MAC: 08:00:27:11:1c:2d DNS: dt2010.itsdept.com NetBIOS: ITSDEPT\DT2010<br>192.168.200.3 - MAC: 00:2e:1f:1f:10:11 DNS: svr8001.itsdept.com NetBIOS: ITSDEPT\SVR8001<br>192.168.200.44 - MAC: 00:2e:1f:1f:b3:1b DNS: svr8037.itsdept.com NetBIOS: ITSDEPT\SVR8037<br>192.168.200.50 - MAC: 00:2e:1f:1f:b3:2e DNS: svr8100.itsdept.com NetBIOS: ITSDEPT\SVR8100 | | | |

| Plugin | Plugin Name | Severity | Family |
|---|---|---|---|
| 18405 | Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness | Medium | Windows |
| The remote version of the Remote Desktop Protocol Server (Terminal / Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP client / makes no effort to validate the identity of the server when setting / up encryption. An attacker with the ability to intercept traffic / from the RDP server can establish encryption with the client and server / without being detected. A MiTM attack of this nature would allow the / attacker to obtain any sensitive information transmitted, including / authentication credentials. / / This flaw exists because the RDP server stores a hardcoded RSA / private key in the mstlsapi.dll library. Any local user with / access to this file (on any Windows system) can retrieve the / key and use it for this attack. | | | |
| **Hosts in Repository 'nocredentials':**<br><br>192.168.10.3 - MAC: 08:00:27:f8:ba:1f DNS: dt0100.itsdept.com NetBIOS: ITSDEPT\DT0100<br>192.168.10.15 - MAC: 08:00:27:f8:ba:2e DNS: dt0109.itsdept.com NetBIOS: ITSDEPT\DT0109<br>192.168.10.23 - MAC: 08:00:27:1e:10:00 DNS: dt0130.itsdept.com NetBIOS: ITSDEPT\DT0130<br>192.168.10.88 - MAC: 08:00:27:09:01:ba DNS: dt0147.itsdept.com NetBIOS: ITSDEPT\DT0147<br>192.168.20.2 - MAC: 08:00:27:11:1c:2d DNS: dt2010.itsdept.com NetBIOS: ITSDEPT\DT2010<br>192.168.200.3 - MAC: 00:2e:1f:1f:10:11 DNS: svr8001.itsdept.com NetBIOS: ITSDEPT\SVR8001<br>192.168.200.44 - MAC: 00:2e:1f:1f:b3:1b DNS: svr8037.itsdept.com NetBIOS: ITSDEPT\SVR8037<br>192.168.200.50 - MAC: 00:2e:1f:1f:b3:2e DNS: svr8100.itsdept.com NetBIOS: ITSDEPT\SVR8100 | | | |

| Plugin | Plugin Name | Severity | Family |
|---|---|---|---|
| 57690 | Terminal Services Encryption Level is Medium or Low | Medium | Misc. |

The remote Terminal Services service is not configured to use strong / cryptography. / / Using weak cryptography with this service may allow an attacker to / eavesdrop on the communications more easily and obtain screenshots / and/or keystrokes.

**Hosts in Repository 'nocredentials':**

192.168.10.3 - MAC: 08:00:27:f8:ba:1f DNS: dt0100.itsdept.com NetBIOS: ITSDEPT\DT0100
192.168.10.15 - MAC: 08:00:27:f8:ba:2e DNS: dt0109.itsdept.com NetBIOS: ITSDEPT\DT0109
192.168.10.23 - MAC: 08:00:27:1e:10:00 DNS: dt0130.itsdept.com NetBIOS: ITSDEPT\DT0130
192.168.10.88 - MAC: 08:00:27:09:01:ba DNS: dt0147.itsdept.com NetBIOS: ITSDEPT\DT0147
192.168.20.2 - MAC: 08:00:27:11:1c:2d DNS: dt2010.itsdept.com NetBIOS: ITSDEPT\DT2010

| Plugin | Plugin Name | Severity | Family |
|---|---|---|---|
| 30218 | Terminal Services Encryption Level is not FIPS-140 Compliant | Low | Misc. |

The encryption setting used by the remote Terminal Services service / is not FIPS-140 compliant.

**Hosts in Repository 'nocredentials':**

192.168.10.3 - MAC: 08:00:27:f8:ba:1f DNS: dt0100.itsdept.com NetBIOS: ITSDEPT\DT0100
192.168.10.15 - MAC: 08:00:27:f8:ba:2e DNS: dt0109.itsdept.com NetBIOS: ITSDEPT\DT0109
192.168.10.23 - MAC: 08:00:27:1e:10:00 DNS: dt0130.itsdept.com NetBIOS: ITSDEPT\DT0130
192.168.10.88 - MAC: 08:00:27:09:01:ba DNS: dt0147.itsdept.com NetBIOS: ITSDEPT\DT0147
192.168.20.2 - MAC: 08:00:27:11:1c:2d DNS: dt2010.itsdept.com NetBIOS: ITSDEPT\DT2010
192.168.200.3 - MAC: 00:2e:1f:1f:10:11 DNS: svr8001.itsdept.com NetBIOS: ITSDEPT\SVR8001
192.168.200.44 - MAC: 00:2e:1f:1f:b3:1b DNS: svr8037.itsdept.com NetBIOS: ITSDEPT\SVR8037
192.168.200.50 - MAC: 00:2e:1f:1f:b3:2e DNS: svr8100.itsdept.com NetBIOS: ITSDEPT\SVR8100