



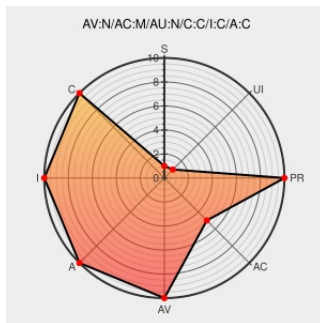
Last Modified on: 03/23/2021 11:23:19 PM UTC

CVE-2011-0029

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

Certain versions of [Remote Desktop Connection Client](#) from [Microsoft](#) contain the following vulnerability:

Untrusted search path vulnerability in the client in Microsoft Remote Desktop Connection 5.2, 6.0, 6.1, and 7.0 allows local users to gain privileges via a Trojan horse DLL in the current working directory, as demonstrated by a directory that contains a .rdp file, aka "Remote Desktop Insecure Library Loading Vulnerability."

CVE-2011-0029 has been assigned by secure@microsoft.com to track the vulnerability

CVSS2 Score: 9.3 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval.org.mitre.oval:def:12480
Windows Remote Desktop Client DLL Loading Error Lets Remote Users Execute Arbitrary Code - SecurityTracker	www.securitytracker.com text/html	 SECTRACK 1025172
US-CERT Technical Cyber Security Alert TA11-067A -- Microsoft Updates for Multiple Vulnerabilities	US Government Resource www.us-cert.gov text/xml	 CERT TA11-067A
Microsoft Security Bulletin MS11-017 - Important Microsoft Docs	docs.microsoft.com text/html	 MS MS11-017
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	 VUPEN ADV-2011-0616

Microsoft Windows Remote Desktop Client Insecure Library Loading Vulnerability - Secunia.com

[web.archive.org](#)
[text/html](#)

 SECUNIA 43628

No Description Provided

[osvdb.org](#)

 OSVDB 71014

Inactive Link

Not Archived

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Remote Desktop Connection Client	5.2	All	All	All
Application	Microsoft	Remote Desktop Connection Client	6.0	All	All	All
Application	Microsoft	Remote Desktop Connection Client	6.1	All	All	All
Application	Microsoft	Remote Desktop Connection Client	7.0	All	All	All
Application	Microsoft	Remote Desktop Connection Client	5.2	All	All	All
Application	Microsoft	Remote Desktop Connection Client	6.0	All	All	All
Application	Microsoft	Remote Desktop Connection Client	6.1	All	All	All
Application	Microsoft	Remote Desktop Connection Client	7.0	All	All	All
Operating System	Microsoft	Windows 2003 Server	All	sp2	All	All
Operating System	Microsoft	Windows 2003 Server	All	sp2	All	All
Operating System	Microsoft	Windows 7	-	All	All	All
Operating System	Microsoft	Windows 7	-	All	All	All
Operating System	Microsoft	Windows Server 2003	All	sp2	All	All
Operating System	Microsoft	Windows Server 2003	All	sp2	All	All
Operating System	Microsoft	Windows Server 2008	All	All	itanium	All
Operating System	Microsoft	Windows Server 2008	All	All	x32	All
Operating System	Microsoft	Windows Server 2008	All	All	x64	All
Operating System	Microsoft	Windows Server 2008	All	sp2	x32	All
Operating System	Microsoft	Windows Server 2008	All	sp2	x64	All

Operating System	Microsoft	Windows Server 2008	All	sp2	x64	All
Operating System	Microsoft	Windows Server 2008	-	sp2	itanium	All
Operating System	Microsoft	Windows Server 2008	r2	All	itanium	All
Operating System	Microsoft	Windows Server 2008	r2	All	x64	All
Operating System	Microsoft	Windows Server 2008	All	All	itanium	All
Operating System	Microsoft	Windows Server 2008	All	All	x32	All
Operating System	Microsoft	Windows Server 2008	All	All	x64	All
Operating System	Microsoft	Windows Server 2008	All	sp2	x32	All
Operating System	Microsoft	Windows Server 2008	All	sp2	x64	All
Operating System	Microsoft	Windows Server 2008	-	sp2	itanium	All
Operating System	Microsoft	Windows Server 2008	r2	All	itanium	All
Operating System	Microsoft	Windows Server 2008	r2	All	x64	All
Operating System	Microsoft	Windows Vista	All	sp1	All	All
Operating System	Microsoft	Windows Vista	All	sp1	x64	All
Operating System	Microsoft	Windows Vista	All	sp2	All	All
Operating System	Microsoft	Windows Vista	All	sp2	x64	All
Operating System	Microsoft	Windows Vista	All	sp1	All	All
Operating System	Microsoft	Windows Vista	All	sp1	x64	All
Operating System	Microsoft	Windows Vista	All	sp2	All	All
Operating System	Microsoft	Windows Vista	All	sp2	x64	All
Operating System	Microsoft	Windows Vista	All	sp1	All	All
Operating System	Microsoft	Windows Vista	All	sp1	x64	All
Operating System	Microsoft	Windows Vista	All	sp2	All	All

Operating System	Microsoft	Windows Vista	All	sp2	x64	All
Operating System	Microsoft	Windows Vista	All	sp1	All	All
Operating System	Microsoft	Windows Vista	All	sp1	x64	All
Operating System	Microsoft	Windows Vista	All	sp2	All	All
Operating System	Microsoft	Windows Vista	All	sp2	x64	All
Operating System	Microsoft	Windows Xp	All	sp3	All	All
Operating System	Microsoft	Windows Xp	All	sp3	All	All
Operating System	Microsoft	Windows Xp	All	sp3	All	All
Operating System	Microsoft	Windows Xp	-	sp2	x64	All
Operating System	Microsoft	Windows Xp	All	sp3	All	All
Operating System	Microsoft	Windows Xp	-	sp2	x64	All
cpe:2.3:a:microsoft:remote_desktop_connection_client:5.2:*:*:*:*:*:						
cpe:2.3:a:microsoft:remote_desktop_connection_client:6.0:*:*:*:*:*:						
cpe:2.3:a:microsoft:remote_desktop_connection_client:6.1:*:*:*:*:*:						
cpe:2.3:a:microsoft:remote_desktop_connection_client:7.0:*:*:*:*:*:						
cpe:2.3:a:microsoft:remote_desktop_connection_client:5.2:*:*:*:*:*:						
cpe:2.3:a:microsoft:remote_desktop_connection_client:6.0:*:*:*:*:*:						
cpe:2.3:a:microsoft:remote_desktop_connection_client:6.1:*:*:*:*:*:						
cpe:2.3:a:microsoft:remote_desktop_connection_client:7.0:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2003_server*:sp2:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2003_server*:sp2:*:*:*:*:						
cpe:2.3:o:microsoft:windows_7:-:*:*:*:*:						
cpe:2.3:o:microsoft:windows_7:-:*:*:*:*:						
cpe:2.3:o:microsoft:windows_server_2003*:sp2:*:*:*:*:						
cpe:2.3:o:microsoft:windows_server_2003*:sp2:*:*:*:*:						
cpe:2.3:o:microsoft:windows_server_2008*:itanium:*:*:*:						

cpe:2.3:o:microsoft:windows_server_2008:*:*:x32:*:*:*:*:
cpe:2.3:o:microsoft:windows_server_2008:*:*:x64:*:*:*:*:
cpe:2.3:o:microsoft:windows_server_2008:*:sp2:x32:*:*:*:*:
cpe:2.3:o:microsoft:windows_server_2008:*:sp2:x64:*:*:*:*:
cpe:2.3:o:microsoft:windows_server_2008:-:sp2:itanium:*:*:*:*:
cpe:2.3:o:microsoft:windows_server_2008:r2:*:itanium:*:*:*:*:
cpe:2.3:o:microsoft:windows_server_2008:r2:*:x64:*:*:*:*:
cpe:2.3:o:microsoft:windows_server_2008:*:*:itanium:*:*:*:*:
cpe:2.3:o:microsoft:windows_server_2008:*:*:x32:*:*:*:*:
cpe:2.3:o:microsoft:windows_server_2008:*:*:x64:*:*:*:*:
cpe:2.3:o:microsoft:windows_server_2008:*:sp2:x32:*:*:*:*:
cpe:2.3:o:microsoft:windows_server_2008:*:sp2:x64:*:*:*:*:
cpe:2.3:o:microsoft:windows_server_2008:-:sp2:itanium:*:*:*:*:
cpe:2.3:o:microsoft:windows_server_2008:r2:*:itanium:*:*:*:*:
cpe:2.3:o:microsoft:windows_server_2008:r2:*:x64:*:*:*:*:
cpe:2.3:o:microsoft:windows_vista:*:sp1:*:*:*:*:
cpe:2.3:o:microsoft:windows_vista:*:sp1:x64:*:*:*:*:
cpe:2.3:o:microsoft:windows_vista:*:sp2:*:*:*:*:
cpe:2.3:o:microsoft:windows_vista:*:sp2:x64:*:*:*:*:
cpe:2.3:o:microsoft:windows_vista:*:sp1:*:*:*:*:
cpe:2.3:o:microsoft:windows_vista:*:sp1:x64:*:*:*:*:
cpe:2.3:o:microsoft:windows_vista:*:sp2:*:*:*:*:
cpe:2.3:o:microsoft:windows_vista:*:sp2:x64:*:*:*:*:
cpe:2.3:o:microsoft:windows_vista:*:sp1:*:*:*:*:
cpe:2.3:o:microsoft:windows_vista:*:sp1:x64:*:*:*:*:
cpe:2.3:o:microsoft:windows_vista:*:sp2:*:*:*:*:
cpe:2.3:o:microsoft:windows_vista:*:sp2:x64:*:*:*:*:
cpe:2.3:o:microsoft:windows_vista:*:sp1:*:*:*:*:
cpe:2.3:o:microsoft:windows_vista:*:sp1:x64:*:*:*:*:
cpe:2.3:o:microsoft:windows_vista:*:sp2:*:*:*:*:
cpe:2.3:o:microsoft:windows_vista:*:sp2:x64:*:*:*:*:
cpe:2.3:o:microsoft:windows_vista:*:sp1:*:*:*:*:
cpe:2.3:o:microsoft:windows_vista:*:sp1:x64:*:*:*:*:

cpe:2.3:o:microsoft:windows_vista:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_vista:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_vista:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_xp:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_xp:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_xp:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_xp:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_xp:-:sp2:x64:*:*:*:*:
cpe:2.3:o:microsoft:windows_xp:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_xp:-:sp2:x64:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© CVE.report 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report