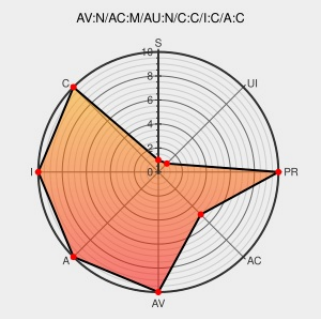
CVE-2009-1133

Published on: 08/12/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:26 PM UTC

CVE-2009-1133

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Windows 2000 from Microsoft contain the following vulnerability:

Heap-based buffer overflow in Microsoft Remote Desktop Connection (formerly Terminal Services Client) running RDP 5.0 through 6.1 on Windows, and Remote Desktop Connection Client for Mac 2.0, allows remote attackers to execute arbitrary code via unspecified parameters, aka "Remote Desktop Connection Heap Overflow Vulnerability."

CVE-2009-1133 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
SecurityTracker.com Archives - Windows Remote Desktop Connection Heap Overflows Let Remote Users Execute Arbitrary Code	www.securitytracker.com, text/html	SECTRACK 1022709
Microsoft Remote Desktop Connection Two Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	Vendor Advisory, web.archive.org, text/html	SECUNIA 36229
Microsoft Security Bulletin MS09-044 - Critical | Microsoft Docs	docs.microsoft.com, text/html	MS MS09-044
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Patch, Vendor Advisory, www.vupen.com, text/html	VUPEN ADV-2009-2238

US-CERT Technical Cyber Security Alert TA09-223A -- Microsoft Updates for Multiple Vulnerabilities	US Government Resource www.us-cert.gov text/xml	CERT TA09-223A
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:5693

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 2000	-	sp4	All	All
Operating System	Microsoft	Windows 2000	-	sp4	All	All
Operating System	Microsoft	Windows Server	2003	sp2	All	All
Operating System	Microsoft	Windows Server	2003	sp2	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	x64	All
Operating System	Microsoft	Windows Server 2008	All	sp2	itanium	All
Operating System	Microsoft	Windows Server 2008	-	-	x32	All
Operating System	Microsoft	Windows Server 2008	-	sp2	x64	All
Operating System	Microsoft	Windows Server 2008	All	All	itanium	All
Operating System	Microsoft	Windows Server 2008	All	All	x64	All
Operating System	Microsoft	Windows Server 2008	All	sp2	itanium	All
Operating System	Microsoft	Windows Server 2008	-	-	x32	All
Operating System	Microsoft	Windows Server 2008	-	sp2	x64	All

Operating System	Microsoft	Windows Vista	All	All	All	All
Operating System	Microsoft	Windows Vista	All	All	x64	All
Operating System	Microsoft	Windows Vista	All	sp1	x64	All
Operating System	Microsoft	Windows Vista	All	sp2	x64	All
Operating System	Microsoft	Windows Vista	-	sp1	All	All
Operating System	Microsoft	Windows Vista	-	sp2	All	All
Operating System	Microsoft	Windows Vista	All	All	All	All
Operating System	Microsoft	Windows Vista	All	All	x64	All
Operating System	Microsoft	Windows Vista	All	sp1	x64	All
Operating System	Microsoft	Windows Vista	All	sp2	x64	All
Operating System	Microsoft	Windows Vista	-	sp1	All	All
Operating System	Microsoft	Windows Vista	-	sp2	All	All
Operating System	Microsoft	Windows Xp	All	sp2	pro_x64	All
Operating System	Microsoft	Windows Xp	-	sp2	All	All
Operating System	Microsoft	Windows Xp	-	sp3	All	All
Operating System	Microsoft	Windows Xp	All	sp2	pro_x64	All
Operating System	Microsoft	Windows Xp	-	sp2	All	All
Operating System	Microsoft	Windows Xp	-	sp3	All	All

cpe:2.3:o:microsoft:windows_2000:-:sp4:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2000:-:sp4:*:*:*:*:*:*:

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_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:*:*:x64:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2008:*:sp2:itanium:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2008:-:-:x32:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2008:-:sp2:x64:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2008:*:*:itanium:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2008:*:*:x64:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2008:*:sp2:itanium:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2008:-:-:x32:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2008:-:sp2:x64:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_vista:*:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_vista:*:*:x64:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_vista:*:sp1:x64:*:*:*:*:*:

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

cpe:2.3:o:microsoft:windows_vista:-:sp1:*:*:*:*:*:*:

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

cpe:2.3:o:microsoft:windows_vista:*:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_vista:*:*:x64:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_vista:*:sp1:x64:*:*:*:*:*:

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

cpe:2.3:o:microsoft:windows_vista:-:sp1:*:*:*:*:*:*:

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

cpe:2.3:o:microsoft:windows_xp:*:sp2:pro_x64:*:*:*:*:*:

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

cpe:2.3:o:microsoft:windows_xp:-:sp3:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:sp2:pro_x64:*:*:*:*:*:

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

cpe:2.3:o:microsoft:windows_xp:-:sp3:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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