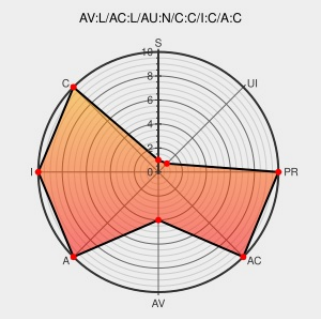
CVE-2005-1207

Published on: 06/14/2005 04:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:24 PM UTC

CVE-2005-1207

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



Certain versions of Windows 2003 Server from Microsoft contain the following vulnerability:

Buffer overflow in the Web Client service in Microsoft Windows XP and Windows Server 2003 allows remote authenticated users to execute arbitrary code via a crafted WebDAV request containing special parameters.

CVE-2005-1207 has been assigned by secure@microsoft.com to track the vulnerability

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	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:721
Secunia - Advisories - Microsoft Windows Web Client Service Vulnerability	Patch Vendor Advisory web.archive.org text/html	SECUNIA 15696
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:1255
Microsoft Security Bulletin MS05-028 - Important | Microsoft Docs	docs.microsoft.com text/html	MS MS05-028

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
Operating System	Microsoft	Windows 2003 Server	r2	All	All	All
Operating System	Microsoft	Windows 2003 Server	r2	All	All	All
Operating System	Microsoft	Windows Xp	All	gold	All	All
Operating System	Microsoft	Windows Xp	All	gold	All	All

cpe:2.3:o:microsoft:windows_2003_server:r2:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:r2:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:gold:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:gold:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→