



CVE-2005-2122

Published on: 10/21/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:28 PM UTC

CVE-2005-2122

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Windows 2000](#) from [Microsoft](#) contain the following vulnerability:

Windows Shell for Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 allows remote attackers to execute arbitrary commands via a shortcut (.lnk) file with long font properties that lead to a buffer overflow in the Client/Server Runtime Server Subsystem (CSRSS), a different vulnerability than CVE-2005-2118.

CVE-2005-2122 has been assigned by secure@microsoft.com to track the vulnerability

CVSS2 Score: **10 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

404 - Not Found

[Vendor Advisory](#)

www.argeniss.com

[application/pdf](#)

[Inactive Link](#) [Not Archived](#)

[MISC](#)

www.argeniss.com/research/MSBugPaper.pdf

US-CERT Vulnerability Note VU#922708

[Third Party Advisory](#)

[US Government Resource](#)

www.kb.cert.org

[text/html](#)

[CERT-VN VU#922708](#)

Microsoft Windows Shell Bugs in Processing '.lnk' Files and in Web View Preview Mode Lets Remote Users Execute Arbitrary Code - SecurityTracker

securitytracker.com

[text/html](#)

[SECTrack 1015040](#)

Repository / Oval Repository

oval.cisecurity.org

[OVAL oval.org/mitre/oval:def:1329](http://oval.org/mitre/oval:def:1329)

	text/html	
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:1488
Secunia - Advisories - Avaya Various Products Multiple Vulnerabilities	Vendor Advisory web.archive.org text/html	 SECUNIA 17172
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:1551
Microsoft Security Bulletin MS05-049 - Important Microsoft Docs	docs.microsoft.com text/html	 MS MS05-049
	support.avaya.com application/pdf	 CONFIRM support.avaya.com/elmodocs2/security/ASA-2005-214.pdf
Secunia - Advisories - Nortel Centrex IP Client Manager Multiple Vulnerabilities	Vendor Advisory web.archive.org text/html	 SECUNIA 17223
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:708
US-CERT Technical Cyber Security Alert TA05-284A -- Microsoft Windows, Internet Explorer, and Exchange Server Vulnerabilities	Third Party Advisory US Government Resource www.us-cert.gov text/html	 CERT TA05-284A
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:1517
Microsoft Windows Malicious Shortcut Handling Remote Code Execution Vulnerability	cve.report (archive) text/html	 BID 15069
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:1537
Secunia - Advisories - Microsoft Windows Shell and Web View Three Vulnerabilities	Vendor Advisory web.archive.org text/html	 SECUNIA 17168

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
Operating System	Microsoft	Windows 2000	All	All	All	All
Operating System	Microsoft	Windows 2000	All	sp1	All	All
Operating System	Microsoft	Windows 2000	All	sp2	All	All
Operating System	Microsoft	Windows 2000	All	sp3	All	All

Operating System	Microsoft	Windows 2000	All	sp3	All	All
Operating System	Microsoft	Windows 2000	All	sp4	All	All
Operating System	Microsoft	Windows 2000	All	All	All	All
Operating System	Microsoft	Windows 2000	All	sp1	All	All
Operating System	Microsoft	Windows 2000	All	sp2	All	All
Operating System	Microsoft	Windows 2000	All	sp3	All	All
Operating System	Microsoft	Windows 2000	All	sp4	All	All
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	All	home	All
Operating System	Microsoft	Windows Xp	All	All	media_center	All
Operating System	Microsoft	Windows Xp	All	gold	professional	All
Operating System	Microsoft	Windows Xp	All	sp1	home	All
Operating System	Microsoft	Windows Xp	All	sp1	media_center	All
Operating System	Microsoft	Windows Xp	All	sp2	tablet_pc	All
Operating System	Microsoft	Windows Xp	All	All	home	All
Operating System	Microsoft	Windows Xp	All	All	media_center	All
Operating System	Microsoft	Windows Xp	All	gold	professional	All
Operating System	Microsoft	Windows Xp	All	sp1	home	All
Operating System	Microsoft	Windows Xp	All	sp1	media_center	All
Operating System	Microsoft	Windows Xp	All	sp2	tablet_pc	All
cpe:2.3:o:microsoft:windows_2000:*****:						
cpe:2.3:o:microsoft:windows_2000:*:sp1:*****:						
cpe:2.3:o:microsoft:windows_2000:*:sp2:*****:						

cpe:2.3:o:microsoft:windows_2000:*:sp3:*:*:*:*:
cpe:2.3:o:microsoft:windows_2000:*:sp4:*:*:*:*:
cpe:2.3:o:microsoft:windows_2000:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_2000:*:sp1:*:*:*:*:
cpe:2.3:o:microsoft:windows_2000:*:sp2:*:*:*:*:
cpe:2.3:o:microsoft:windows_2000:*:sp3:*:*:*:*:
cpe:2.3:o:microsoft:windows_2000:*:sp4:*:*:*:*:
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:*:*:home:*:*:*:
cpe:2.3:o:microsoft:windows_xp:*:*:media_center:*:*:*:
cpe:2.3:o:microsoft:windows_xp:*:gold:professional:*:*:*:
cpe:2.3:o:microsoft:windows_xp:*:sp1:home:*:*:*:
cpe:2.3:o:microsoft:windows_xp:*:sp1:media_center:*:*:*:
cpe:2.3:o:microsoft:windows_xp:*:sp2:tablet_pc:*:*:*:
cpe:2.3:o:microsoft:windows_xp:*:*:home:*:*:*:
cpe:2.3:o:microsoft:windows_xp:*:*:media_center:*:*:*:
cpe:2.3:o:microsoft:windows_xp:*:gold:professional:*:*:*:
cpe:2.3:o:microsoft:windows_xp:*:sp1:home:*:*:*:
cpe:2.3:o:microsoft:windows_xp:*:sp1:media_center:*:*:*:
cpe:2.3:o:microsoft:windows_xp:*:sp2:tablet_pc:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

[site](#). This site includes MITRE data granted under the following [license](#).

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