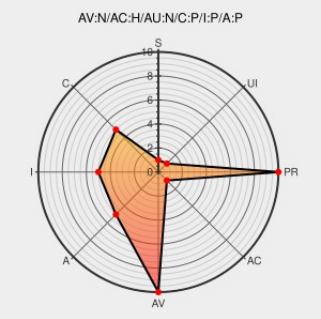
CVE-2004-1049

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:10 PM UTC

CVE-2004-1049

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



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

Integer overflow in the LoadImage API of the USER32 Lib for Microsoft Windows allows remote attackers to execute arbitrary code via a .bmp, .cur, .ico or .ani file with a large image size field, which leads to a buffer overflow, aka the "Cursor and Icon Format Handling Vulnerability."

CVE-2004-1049 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5.1 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
404 Not Found	Exploit, web.archive.org, text/html, Inactive Link, Not Archived	MISC www.xfocus.net/flashsky/icoExp/index.html
US-CERT Technical Cyber Security Alert TA05-012A -- Multiple Vulnerabilities in Microsoft Windows Icon and Cursor Processing	Third Party Advisory, US Government Resource, www.us-cert.gov, text/html	CERT TA05-012A
Repository / Oval Repository	oval.cisecurity.org, text/html	OVAL oval:org.mitre.oval:def:2956
Secunia - Advisories - Microsoft Windows Multiple Vulnerabilities	web.archive.org, text/html	SECUNIA 13645
'Microsoft Windows LoadImage API Integer Buffer overflow' -	marc.info	BUGTRAQ 20041223 Microsoft

MARC	application/octet-stream	Windows LoadImage API Integer Buffer overflow
SecurityTracker.com Archives - Microsoft Windows LoadImage API Buffer Overflow Lets Remote Users Execute Arbitrary Code	securitytracker.com text/html	SECTRACK 1012684
Microsoft Windows LoadImage API Function Integer Overflow Vulnerability	cve.report (archive) text/html	BID 12095
No Description Provided	web.archive.org text/html Inactive Link Not Archived	CIAC P-094
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 12623
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:4671
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:3220
US-CERT Vulnerability Note VU#625856	Third Party Advisory US Government Resource www.kb.cert.org text/html	CERT-VN VU#625856
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:3097
Microsoft Security Bulletin MS05-002 - Critical | Microsoft Docs	docs.microsoft.com text/html	MS MS05-002
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF win-loadimage-bo(18668)
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:3355

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	Microsoft	Windows 2000	All	sp4	All	fr

System						
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	fr
Operating System	Microsoft	Windows 2003 Server	r2	All	All	All
Operating System	Microsoft	Windows 2003 Server	r2	All	All	All
Operating System	Microsoft	Windows Nt	All	All	All	All
Operating System	Microsoft	Windows Nt	All	All	All	All
Operating System	Microsoft	Windows Xp	All	gold	All	All
Operating System	Microsoft	Windows Xp	All	sp1	tablet_pc	All
Operating System	Microsoft	Windows Xp	All	gold	All	All
Operating System	Microsoft	Windows Xp	All	sp1	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:*:fr:*:*:*:*:

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:*:fr:*:*:*:*:

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

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

cpe:2.3:o:microsoft:windows_nt:*:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:*:*:*:*:*:*:*:*:

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

cpe:2.3:o:microsoft:windows_xp:*:sp1:tablet_pc:*:*:*:*:*:

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

cpe:2.3:o:microsoft:windows_xp:*:sp1:tablet_pc:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→