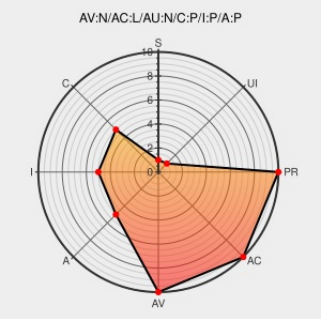
CVE-2003-0812

Published on: 11/18/2003 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:45 PM UTC

CVE-2003-0812

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



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

Stack-based buffer overflow in a logging function for Windows Workstation Service (WKSSVC.DLL) allows remote attackers to execute arbitrary code via RPC calls that cause long entries to be written to a debug log file ("NetSetup.LOG"), as demonstrated using the NetAddAlternateComputerName API.

CVE-2003-0812 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Cisco - Networking, Cloud, and Cybersecurity Solutions	www.cisco.com text/html	CISCO 20040129 Buffer Overrun in Microsoft Windows 2000 Workstation Service (MS03-049)
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:575
'EEYE: Windows Workstation Service Remote Buffer Overflow' - MARC	marc.info text/html	BUGTRAQ 20031111 EEYE: Windows Workstation Service Remote Buffer Overflow
Microsoft Windows Workstation Service Remote Buffer Overflow Vulnerability	Exploit Patch Vendor Advisory cve.report (archive) text/html	BID 9011

'Proof of concept for Windows Workstation Service overflow' - MARC	marc.info text/x-c	BUGTRAQ 20031112 Proof of concept for Windows Workstation Service overflow
Microsoft Security Bulletin MS03-049 - Critical | Microsoft Docs	docs.microsoft.com text/html	MS MS03-049
CERT/CC Vulnerability Note VU#567620	Patch Third Party Advisory US Government Resource www.kb.cert.org text/html	CERT-VN VU#567620
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:331
CERT Advisory CA-2003-28 Buffer Overflow in Windows Workstation Service	US Government Resource www.cert.org text/html	CERT CA-2003-28

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	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 Xp	All	All	64-bit	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	64-bit	All
Operating System	Microsoft	Windows Xp	All	sp1	home	All
Operating System	Microsoft	Windows Xp	All	All	64-bit	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	64-bit	All
Operating System	Microsoft	Windows Xp	All	sp1	home	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_xp:*:*:64-bit:*:*:*:*:*:

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:*:sp1:64-bit:*:*:*:*:*:

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

cpe:2.3:o:microsoft:windows_xp:*:*:64-bit:*:*:*:*:*:

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:*:sp1:64-bit:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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