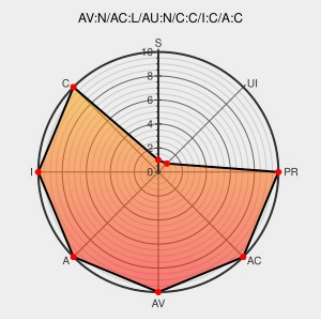
CVE-2004-1080

Published on: 12/01/2004 12:00:00 AM UTC

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

CVE-2004-1080

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



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

The WINS service (wins.exe) on Microsoft Windows NT Server 4.0, Windows 2000 Server, and Windows Server 2003 allows remote attackers to write to arbitrary memory locations and possibly execute arbitrary code via a modified memory pointer in a WINS replication packet to TCP port 42, aka the "Association Context Vulnerability."

CVE-2004-1080 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 10 - HIGH

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

CVE References

Description	Tags	Link
(Vendor Issues Fix) Microsoft WINS Memory Overwrite Lets Remote Users Execute Arbitary Code - SecurityTracker	securitytracker.com text/html	SECTRACK 1012516
How to help protect against a WINS security issue	support.microsoft.com text/html	MSKB 890710
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:1549
Microsoft Security Bulletin MS04-045 - Important | Microsoft Docs	docs.microsoft.com text/html	MS MS04-045
Secunia - Advisories - Microsoft Windows WINS Replication Packet Handling Vulnerability	web.archive.org text/html	SECUNIA 13328

Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:3677
404 Not Found	www.immunitysec.com application/pdf Inactive Link Not Archived	MISC www.immunitysec.com/downloads/instantanea.pdf
No Description Provided	web.archive.org text/html Inactive Link Not Archived	ISS 20041129 Microsoft WINS Server Vulnerability
US-CERT Vulnerability Note VU#145134	Patch Third Party Advisory US Government Resource www.kb.cert.org text/html	CERT-VN VU#145134
'Immunity, Inc Advisor' - MARC	marc.info text/html	BUGTRAQ 20041126 Immunity, Inc Advisor
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:4372
No Description Provided	web.archive.org text/html Inactive Link Not Archived	CIAC P-054
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:2541
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 12378
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:2734
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF wins-memory-pointer-hijack(18259)
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:4831
Microsoft Windows WINS Association Context Data Remote Memory Corruption Vulnerability	Patch Vendor Advisory cve.report (archive) text/html	BID 11763

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 2003 Server	2000	All	small_business_server	All
Operating System	Microsoft	Windows 2003 Server	2003	All	small_business_server	All
Operating System	Microsoft	Windows 2003 Server	enterprise	All	64-bit	All
Operating System	Microsoft	Windows 2003 Server	enterprise_64-bit	All	All	All
Operating System	Microsoft	Windows 2003 Server	r2	All	64-bit	All
Operating System	Microsoft	Windows 2003 Server	r2	All	datacenter_64-bit	All
Operating System	Microsoft	Windows 2003 Server	standard	All	64-bit	All
Operating System	Microsoft	Windows 2003 Server	web	All	All	All
Operating System	Microsoft	Windows 2003 Server	2000	All	small_business_server	All
Operating System	Microsoft	Windows 2003 Server	2003	All	small_business_server	All
Operating System	Microsoft	Windows 2003 Server	enterprise	All	64-bit	All
Operating System	Microsoft	Windows 2003 Server	enterprise_64-bit	All	All	All
Operating System	Microsoft	Windows 2003 Server	r2	All	64-bit	All
Operating System	Microsoft	Windows 2003 Server	r2	All	datacenter_64-bit	All
Operating System	Microsoft	Windows 2003 Server	standard	All	64-bit	All

System						
Operating System	Microsoft	Windows 2003 Server	web	All	All	All
Operating System	Microsoft	Windows Nt	4.0	All	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	All	server	All
Operating System	Microsoft	Windows Nt	4.0	All	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp1	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp1	server	All
Operating System	Microsoft	Windows Nt	4.0	sp1	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp2	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp2	server	All
Operating System	Microsoft	Windows Nt	4.0	sp2	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp3	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp3	server	All
Operating System	Microsoft	Windows Nt	4.0	sp3	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp4	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp4	server	All
Operating System	Microsoft	Windows Nt	4.0	sp4	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp5	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp5	server	All
Operating System	Microsoft	Windows Nt	4.0	sp5	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp6	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp6	server	All
Operating System	Microsoft	Windows Nt	4.0	sp6	terminal_server	All
Operating	Microsoft	Windows Nt	4.0	sp6a	enterprise_server	All

System						
Operating System	Microsoft	Windows Nt	4.0	sp6a	server	All
Operating System	Microsoft	Windows Nt	4.0	sp6a	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	All	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	All	server	All
Operating System	Microsoft	Windows Nt	4.0	All	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp1	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp1	server	All
Operating System	Microsoft	Windows Nt	4.0	sp1	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp2	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp2	server	All
Operating System	Microsoft	Windows Nt	4.0	sp2	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp3	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp3	server	All
Operating System	Microsoft	Windows Nt	4.0	sp3	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp4	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp4	server	All
Operating System	Microsoft	Windows Nt	4.0	sp4	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp5	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp5	server	All
Operating System	Microsoft	Windows Nt	4.0	sp5	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp6	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp6	server	All
Operating	Microsoft	Windows Nt	4.0	sp6	terminal_server	All

System						
Operating System	Microsoft	Windows Nt	4.0	sp6a	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp6a	server	All
Operating System	Microsoft	Windows Nt	4.0	sp6a	terminal_server	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:2000:*:small_business_server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:2003:*:small_business_server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:enterprise:*:64-bit:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:enterprise_64-bit:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:r2:*:64-bit:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:r2:*:datacenter_64-bit:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:standard:*:64-bit:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:web:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:2000:*:small_business_server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:2003:*:small_business_server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:enterprise:*:64-bit:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:enterprise_64-bit:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:r2:*:64-bit:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:r2:*:datacenter_64-bit:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:standard:*:64-bit:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:web:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:*:enterprise_server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:*:server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:*:terminal_server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp1:enterprise_server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp1:server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp1:terminal_server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp2:enterprise_server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp2:server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp2:terminal_server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp3:enterprise_server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp3:server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp3:terminal_server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp4:enterprise_server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp4:server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp4:terminal_server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp5:enterprise_server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp5:server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp5:terminal_server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp6:enterprise_server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp6:server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp6:terminal_server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp6a:enterprise_server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp6a:server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp6a:terminal_server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:*:enterprise_server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:*:server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:*:terminal_server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp1:enterprise_server:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp1:server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp1:terminal_server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp2:enterprise_server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp2:server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp2:terminal_server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp3:enterprise_server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp3:server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp3:terminal_server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp4:enterprise_server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp4:server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp4:terminal_server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp5:enterprise_server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp5:server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp5:terminal_server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp6:enterprise_server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp6:server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp6:terminal_server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp6a:enterprise_server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp6a:server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp6a:terminal_server:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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