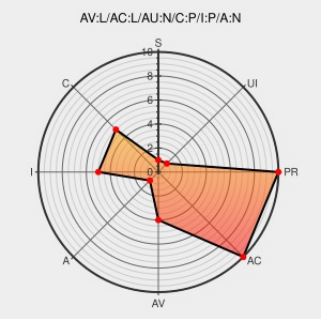
CVE-2002-2401

Published on: 12/31/2002 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:05 PM UTC

CVE-2002-2401

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



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

NT Virtual DOS Machine (NTVDM.EXE) in Windows 2000, NT and XP does not verify user execution permissions for 16-bit executable files, which allows local users to bypass the loader and execute arbitrary programs.

CVE-2002-2401 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 3.6 - LOW

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

CVE References

Description	Tags	Link
ISS X-Force Database: win-execute-permissions-16bit (10132): Windows fails to properly check execute permissions for 16-bit executable files	web.archive.org, text/html, Inactive Link, Not Archived	XF win-execute-permissions-16bit(10132)
No Description Provided	web.archive.org, text/html, Inactive Link, Not Archived	MISC www.abtrusion.com/msexe16.asp
Software Restriction Policies Do Not Recognize 16-Bit Programs	support.microsoft.com, text/html	MSKB 319458
Windows 2000/NT/XP 16-bit Application Permission Bypass Vulnerability	cve.report (archive), text/html	BID 5740
No Description Provided	archives.neohapsis.com, Inactive Link, Not Archived	BUGTRAQ 20020918 Execution Rights Not Checked Correctly For 16-bit Applications

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	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 Nt	4.0	All	All	All
Operating System	Microsoft	Windows Nt	4.0	All	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp1	enterprise	All
Operating System	Microsoft	Windows Nt	4.0	sp1	server	All
Operating System	Microsoft	Windows Nt	4.0	sp1	terminal_srv	All
Operating System	Microsoft	Windows Nt	4.0	sp1	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp2	enterprise	All
Operating System	Microsoft	Windows Nt	4.0	sp2	server	All
Operating System	Microsoft	Windows Nt	4.0	sp2	terminal_srv	All
Operating System	Microsoft	Windows Nt	4.0	sp2	workstation	All

System						
Operating System	Microsoft	Windows Nt	4.0	sp3	enterprise	All
Operating System	Microsoft	Windows Nt	4.0	sp3	server	All
Operating System	Microsoft	Windows Nt	4.0	sp3	terminal_srv	All
Operating System	Microsoft	Windows Nt	4.0	sp3	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp4	enterprise	All
Operating System	Microsoft	Windows Nt	4.0	sp4	server	All
Operating System	Microsoft	Windows Nt	4.0	sp4	terminal_srv	All
Operating System	Microsoft	Windows Nt	4.0	sp4	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp5	enterprise	All
Operating System	Microsoft	Windows Nt	4.0	sp5	server	All
Operating System	Microsoft	Windows Nt	4.0	sp5	terminal_srv	All
Operating System	Microsoft	Windows Nt	4.0	sp5	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp6	enterprise	All
Operating System	Microsoft	Windows Nt	4.0	sp6	server	All
Operating System	Microsoft	Windows Nt	4.0	sp6	terminal_srv	All
Operating System	Microsoft	Windows Nt	4.0	sp6	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp6a	enterprise	All
Operating System	Microsoft	Windows Nt	4.0	sp6a	server	All
Operating System	Microsoft	Windows Nt	4.0	sp6a	workstation	All
Operating System	Microsoft	Windows Nt	4.0	All	All	All
Operating System	Microsoft	Windows Nt	4.0	All	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp1	enterprise	All
Operating System	Microsoft	Windows Nt	4.0	sp1	server	All

System						
Operating System	Microsoft	Windows Nt	4.0	sp1	terminal_srv	All
Operating System	Microsoft	Windows Nt	4.0	sp1	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp2	enterprise	All
Operating System	Microsoft	Windows Nt	4.0	sp2	server	All
Operating System	Microsoft	Windows Nt	4.0	sp2	terminal_srv	All
Operating System	Microsoft	Windows Nt	4.0	sp2	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp3	enterprise	All
Operating System	Microsoft	Windows Nt	4.0	sp3	server	All
Operating System	Microsoft	Windows Nt	4.0	sp3	terminal_srv	All
Operating System	Microsoft	Windows Nt	4.0	sp3	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp4	enterprise	All
Operating System	Microsoft	Windows Nt	4.0	sp4	server	All
Operating System	Microsoft	Windows Nt	4.0	sp4	terminal_srv	All
Operating System	Microsoft	Windows Nt	4.0	sp4	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp5	enterprise	All
Operating System	Microsoft	Windows Nt	4.0	sp5	server	All
Operating System	Microsoft	Windows Nt	4.0	sp5	terminal_srv	All
Operating System	Microsoft	Windows Nt	4.0	sp5	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp6	enterprise	All
Operating System	Microsoft	Windows Nt	4.0	sp6	server	All
Operating System	Microsoft	Windows Nt	4.0	sp6	terminal_srv	All
Operating System	Microsoft	Windows Nt	4.0	sp6	workstation	All
Operating	Microsoft	Windows Nt	4.0	sp6a	enterprise	All

System						
Operating System	Microsoft	Windows Nt	4.0	sp6a	server	All
Operating System	Microsoft	Windows Nt	4.0	sp6a	workstation	All
Operating System	Microsoft	Windows Xp	All	All	home	All
Operating System	Microsoft	Windows Xp	All	All	pro	All
Operating System	Microsoft	Windows Xp	All	sp1	home	All
Operating System	Microsoft	Windows Xp	All	sp1	pro	All
Operating System	Microsoft	Windows Xp	All	All	home	All
Operating System	Microsoft	Windows Xp	All	All	pro	All
Operating System	Microsoft	Windows Xp	All	sp1	home	All
Operating System	Microsoft	Windows Xp	All	sp1	pro	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:*:*:*:*:*:*:*:*:

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_nt:4.0:*:*:*:*:*:*:*:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

cpe:2.3:o:microsoft:windows_xp:*:*:pro:*:*:*:*:*:

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

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

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

cpe:2.3:o:microsoft:windows_xp:*:*:pro:*:*:*:*:*:

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→