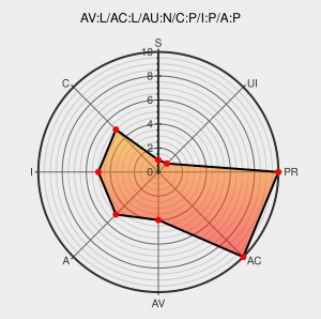
CVE-2002-1230

Published on: 11/04/2002 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:01 PM UTC

CVE-2002-1230

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



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

NetDDE Agent on Windows NT 4.0, 4.0 Terminal Server Edition, Windows 2000, and Windows XP allows local users to execute arbitrary code as LocalSystem via "shatter" style attack by sending a WM_COPYDATA message followed by a WM_TIMER message, as demonstrated by GetAd, aka "Flaw in Windows WM_TIMER Message Handling Could Enable Privilege Elevation."

CVE-2002-1230 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.6 - MEDIUM

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

CVE References

Description	Tags	Link
ISS X-Force Database: win-netdde-gain-privileges (10343): Windows NetDDE Agent can be used to gain elevated privileges	Vendor Advisory, web.archive.org, text/html, Inactive Link, Not Archived	XF win-netdde-gain-privileges(10343)
No Description Provided	getad.chat.ru, text/html	MISC getad.chat.ru/
Microsoft Windows NetDDE Privilege Escalation Vulnerability	cve.report (archive), text/html	BID 5927
Repository / Oval Repository	oval.cisecurity.org, text/html	OVAL oval:org.mitre.oval:def:681

Microsoft Security Bulletin MS02-071 - Important | Microsoft Docs	docs.microsoft.com text/html	MS MS02-071
No Description Provided	web.archive.org text/html Inactive Link Not Archived	CIAC N-027
.:[packet storm]:. - http://packetstormsecurity.org/	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	MISC www.packetstormsecurity.nl/filedesc/GetAd.c.html

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

Operating System	Microsoft	Windows 2000 Terminal Services	All	sp2	All	All
Operating System	Microsoft	Windows 2000 Terminal Services	All	sp3	All	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_2000_terminal_services:*:*:*:*:*:*:*:*:
- cpe:2.3:o:microsoft:windows_2000_terminal_services:*:sp1:*:*:*:*:*:*:
- cpe:2.3:o:microsoft:windows_2000_terminal_services:*:sp2:*:*:*:*:*:*:
- cpe:2.3:o:microsoft:windows_2000_terminal_services:*:sp3:*:*:*:*:*:*:
- cpe:2.3:o:microsoft:windows_2000_terminal_services:*:*:*:*:*:*:*:*:
- cpe:2.3:o:microsoft:windows_2000_terminal_services:*:sp1:*:*:*:*:*:*:
- cpe:2.3:o:microsoft:windows_2000_terminal_services:*:sp2:*:*:*:*:*:*:
- cpe:2.3:o:microsoft:windows_2000_terminal_services:*:sp3:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→