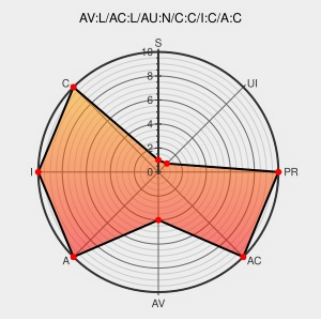
CVE-2004-2339

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

Last Modified on: 03/23/2021 11:28:13 PM UTC

CVE-2004-2339

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



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

** DISPUTED ** Microsoft Windows 2000, XP, and possibly 2003 allows local users with the SeDebugPrivilege privilege to execute arbitrary code as kernel and read or write kernel memory via the NtSystemDebugControl function, which does not verify its pointer arguments. Note: this issue has been disputed, since Administrator privileges are typically required to exploit this issue, thus privilege boundaries are not crossed.

CVE-2004-2339 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.2 - HIGH

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

CVE References

Description	Tags	Link
Windows XP Kernel NtSystemDebugControl() Flaws Let Local Users With SeDebugPrivilege Execute Arbitrary Code in Kernel Mode - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1009128
Neohapsis Archives - Bugtraq - #0529 - RE: Multiple WinXP kernel vulns can give user mode programs kernel mode privileges	web.archive.org text/html Inactive Link Not Archived	BUGTRAQ 20040219 RE: Multiple WinXP kernel vulns can give user mode programs kernel mode privileges
No Description Provided	web.archive.org text/html Inactive Link Not Archived	BUGTRAQ 20040219 RE: Multiple WinXP kernel vulns can give user mode programs kernel mode privileges

IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF win-kernel-gain-privileges(15263)
SecurityFocus	Vendor Advisory www.securityfocus.com text/html	BUGTRAQ 20040218 Multiple WinXP kernel vulns can give user mode programs kernel mode privileges

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	All	All	All
Operating System	Microsoft	Windows 2003 Server	r2	All	All	All
Operating System	Microsoft	Windows 2003 Server	r2	All	All	All
Operating System	Microsoft	Windows Xp	All	gold	All	All
Operating System	Microsoft	Windows Xp	All	gold	All	All

cpe:2.3:o:microsoft:windows_2000:*:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2000:*:*:*:*:*:*:*:*:

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

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

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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