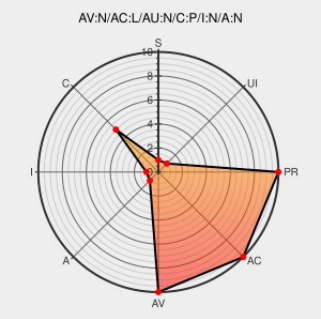
CVE-2005-2150

Published on: 07/11/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:27 PM UTC

CVE-2005-2150

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



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

Windows NT 4.0 and Windows 2000 before URP1 for Windows 2000 SP4 does not properly prevent NULL sessions from accessing certain alternate named pipes, which allows remote attackers to (1) list Windows services via svcctl or (2) read eventlogs via eventlog.

CVE-2005-2150 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Microsoft Windows Named Pipe NULL Session Bugs in svcctl and eventlog RPC Interfaces Disclose Information to Remote Users - SecurityTracker	securitytracker.com, text/html	SECTRACK 1014417
Microsoft Windows MSRPC Eventlog Information Disclosure Vulnerability	cve.report (archive), text/html	BID 14178
404 Not Found	web.archive.org, text/html, Inactive Link, Not Archived	MISC www.hsc.fr/ressources/presentations/null_sessions/
Microsoft Windows MSRPC SVCCTL Service Enumeration Vulnerability	cve.report (archive), text/html	BID 14177
Secunia - Advisories - Windows Anonymous Named Pipe Connection Information Disclosure	web.archive.org, text/html	SECUNIA 14189

No Description Provided	marc.info text/html	BUGTRAQ 20050707 NULL sessions vulnerabilities using alternate named pipes
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF win-name-pipe-null-information-disclosure(21286)
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF win-pipe-null-eventlog-information-disclosure(21288)

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 Nt	4.0	All	All	All
Operating System	Microsoft	Windows Nt	4.0	All	All	All

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

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

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→