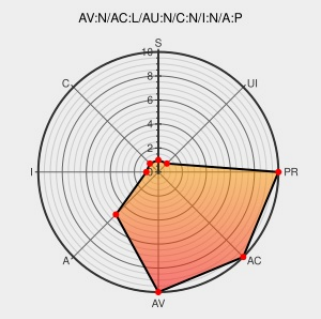
CVE-2005-2804

Published on: 10/04/2005 12:00:00 AM UTC

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

CVE-2005-2804

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



Certain versions of Groupwise from Novell contain the following vulnerability:

Integer overflow in the registry parsing code in GroupWise 6.5.3, and possibly earlier version, allows remote attackers to cause a denial of service (application crash) via a large TCP/IP port in the Windows registry key.

CVE-2005-2804 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**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
SecurityTracker.com Archives - Novell GroupWise Client Integer Overflow in Processing 'IP Port' Registry Key May Let Local Users Execute Arbitrary Code	securitytracker.com, text/html	SECTRACK 1014977
Novell GroupWise Client Local Integer Overflow Vulnerability	Exploit, Patch, cve.report (archive), text/html	BID 14952
[Full-disclosure] [ISR] - Novell GroupWise Client Integer	Patch, Vendor Advisory	FULLDISC 20050927 [ISR] - Novell GroupWise Client Integer Overflow

Client Integer Overflow	web.archive.org text/html Inactive Link Not Archived	
No Description Provided	support.novell.com text/html	CONFIRM support.novell.com/cgi-bin/search/searchtid.cgi?/10098814.htm
'[ISR] - Novell GroupWise Client Integer Overflow' - MARC	marc.info text/html	BUGTRAQ 20050927 [ISR] - Novell GroupWise Client Integer Overflow
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF novell-groupwise-port-number-overflow(22419)
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 19862
Novell GroupWise Client Integer Overflow - CXSecurity.com	securityreason.com text/html	SREASON 28
HTTP 404 Page Not Found	Patch Vendor Advisory support.novell.com text/html Inactive Link Not Archived	CONFIRM support.novell.com/techcenter/search/search.do?cmd=displayKC&docType=%20c&externalId=10098814html&sliceId=&dialogID=7171
No Description Provided	archives.neohapsis.com Inactive Link Not Archived	FULLDISC 20050927 Re: [ISR] - Novell GroupWise Client Integer Overflow
ISR, Infobyte Security Research	web.archive.org text/html Inactive Link Not Archived	MISC www.infobyte.com.ar/adv/ISR-13.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Novell	Groupwise	6.5.3	All	All	All
Application	Novell	Groupwise	6.5.3	All	All	All

cpe:2.3:a:novell:groupwise:6.5.3:*:*:*:*:*:*:*:

cpe:2.3:a:novell:groupwise:6.5.3:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→