CVE-2005-1543

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2005-1543
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-05-25 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Multiple stack-based and heap-based buffer overflows in Remote Management authentication (zenrem32.exe) on Novell ZE

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:P/I:P/A:P

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Novell	Zenworks	6.5	All	All	All

Application	Novell	Zenworks Desktops	3.2	sp2	All	All
Application	Novell	Zenworks Desktops	4.0	All	All	All
Application	Novell	Zenworks Desktops	4.0.1	All	All	All
Application	Novell	Zenworks Remote Management	All	All	All	All
Application	Novell	Zenworks Servers	3.2	All	All	All
Application	Novell	Zenworks Server Management	6.5	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
support.novell.com/cgi-bin/search/searchtid.cgi
Secunia - Advisories - Novell ZENworks Remote Management Buffer Overflows
'NOVELL ZENWORKS MULTIPLE =?utf-8?Q?REM=C3=98TE?= STACK & HEAP OVERFLOWS' - MARC
Novell ZENworks Multiple Remote Pre-Authentication Buffer Overflow Vulnerabilities
IBM X-Force Exchange
SecurityTracker.com Archives - Novell ZENworks Remote Management Buffer Overflows in Authentication Protocol Let Remote Users Execut
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
rem0te.com
IBM X-Force Exchange
IBM X-Force Exchange
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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