

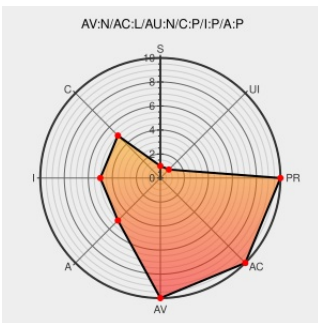


CVE-2005-3655

Published on: 12/31/2005 05:00:00 AM UTC

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

CVE-2005-3655

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Open Enterprise Server](#) from [Novell](#) contain the following vulnerability:

Heap-based buffer overflow in Novell Open Enterprise Server Remote Manager (novell-nrm) in Novell SUSE Linux Enterprise Server 9 allows remote attackers to execute arbitrary code via an HTTP POST request with a negative Content-Length parameter.

CVE-2005-3655 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

CXSecurity - IDS

[securityreason.com](#)
[text/html](#)

[SREASON 348](#)

SuSE Open Enterprise Server Novell Remote Manager HTTP Request Header Heap Overflow Vulnerability

[cve.report \(archive\)](#)
[text/html](#)

[BID 16226](#)

Secunia - Advisories - Novell Open Enterprise Server Remote Manager Buffer Overflow

[web.archive.org](#)
[text/html](#)

[SECUNIA 18484](#)

No Description Provided

[www.osvdb.org](#)

[OSVDB 22455](#)

Inactive Link **Not Archived**

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

[XF novell-remote-manager-bo\(24111\)](#)

Accenture | Let there be change

[Exploit](#)

[IDEFENSE 20060113 Novell](#)

www.iddefense.com

text/html

SUSE Linux Enterprise Server Remote Manager Heap Overflow

web.archive.org

text/html

ot SUSE SUSE-SA:2006:002

securitytracker.com

text/html

SECTrack 1015487

Security Announcement

Novell Remote Manager for SUSE Linux Content-Length Heap Overflow Lets Remote Users Execute Arbitrary Code - SecurityTracker

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
Application	Novell	Open Enterprise Server	9	All	All	All
Application	Novell	Open Enterprise Server	9	All	All	All

cpe:2.3:a:novell:open_enterprise_server:9:*:*:*:*:*:

cpe:2.3:a:novell:open_enterprise_server:9:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →

© CVE.report 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)