



CVE-2006-6306

Published on: 12/05/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:04 PM UTC

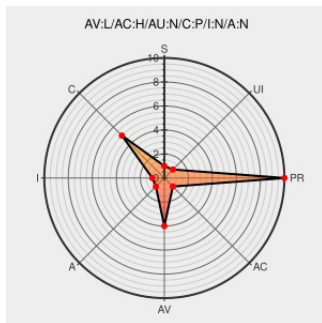
CVE-2006-6306

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Client](#) from [Novell](#) contain the following vulnerability:

Format string vulnerability in Novell Modular Authentication Services (NMAS) in the Novell Client 4.91 SP2 and SP3 allows users with physical access to read stack and memory contents via format string specifiers in the Username field of the logon window.

CVE-2006-6306 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **1.2 - LOW**

Access Vector

LOCAL

Access Complexity

HIGH

Authentication

NONE

Confidentiality Impact

PARTIAL

Integrity Impact

NONE

Availability Impact

NONE

CVE References

Description

Tags

Link

Novell Client NMAS Login Prompt Format String Weakness - Secunia Advisories - Vulnerability Intelligence - Secunia.com

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

[X](#) [SECUNIA 23363](#)

Layered Defense Security Advisories

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

[MISC](#) www.layereddefense.com/Novell01DEC.html

[Inactive Link](#) [Not Archived](#)

SecurityReason - Novell Client 4.91 Format String Vulnerability

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

[CX](#) [SREASON 1970](#)

Novell Modular Authentication Service

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

[G](#) [SECTRACK 1017377](#)

Authentication Service Format String Flaw Has Unspecified Impact - SecurityTracker	text/html	
No Description Provided	support.novell.com text/html Inactive Link Not Archived	CONFIRM support.novell.com/cgi-bin/search/searchtid.cgi?/2974876.htm
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2006-4987
No Description Provided	support.novell.com text/html Inactive Link Not Archived	CONFIRM support.novell.com/cgi-bin/search/searchtid.cgi?/2974872.htm
[Full-disclosure] Layered Defense Advisory: Novell Client 4.91 Format String Vulnerability	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	FULLDISC 20061201 Layered Defense Advisory: Novell Client 4.91 Format String Vulnerability
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF novell-nmas-format-string(30644)
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20061201 Layered Defense Advisory: Novell Client 4.91 Format String Vulnerability
No Description Provided	secure-support.novell.com Inactive Link Not Archived	CONFIRM secure-support.novell.com/KanisaPlatform/Publishing/372/3546910_f.SAL_Public.html

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	Client	4.91	sp2	All	All
Application	Novell	Client	4.91	sp3	All	All
Application	Novell	Client	4.91	sp2	All	All
Application	Novell	Client	4.91	sp3	All	All
cpe:2.3:a:novell:client:4.91:sp2:****:*.:						
cpe:2.3:a:novell:client:4.91:sp3:****:*.:						
cpe:2.3:a:novell:client:4.91:sp2:****:*.:						
cpe:2.3:a:novell:client:4.91:sp3:****:*.:						

No vendor comments have been submitted for this CVE

© [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](#)