



CVE-2006-2304

Published on: 05/11/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:08 PM UTC

CVE-2006-2304

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

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

Multiple integer overflows in the DPRPC library (DPRPCW32.DLL) in Novell Client 4.83 SP3, 4.90 SP2 and 4.91 SP2 allow remote attackers to execute arbitrary code via an XDR encoded array with a field that specifies a large number of elements, which triggers the overflows in the ndps_xdr_array function. NOTE: this was originally reported to be a buffer overflow by Novell, but the original cause is an integer overflow.

CVE-2006-2304 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **10 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

[www.vupen.com](#)
[text/html](#)

[VUPEN ADV-2006-1759](#)

SecurityFocus

[www.securityfocus.com](#)
[text/html](#)

[BUGTRAQ 20060515 Novell NDPS Remote Vulnerability \(Server & Client\)](#)

SecurityTracker.com Archives - Novell Client Buffer Overflow in 'DPRPCW32.DLL' Lets Remote Users Execute Arbitrary Code

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

[SECTRAK 1016052](#)

Secunia - Advisories - Novell Distributed Print Services Integer Overflow Vulnerability

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

[SECUNIA 20048](#)

IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF novell-ndps-overflow(26314)
No Description Provided	www.osvdb.org Inactive Link Not Archived	 OSVDB 25429
Novell Client Unspecified Buffer Overflow Vulnerability	Patch cve.report (archive) text/html	 BID 17931
[Full-Disclosure] Mailing List Charter	lists.grok.org.uk text/html Inactive Link Not Archived	 FULLDISC 20060515 Novell NDPS Remote Vulnerability (Server & Client)
Support Document Not Found	Patch web.archive.org text/html Inactive Link Not Archived	 CONFIRM support.novell.com/cgi-bin/search/searchtid.cgi?/2973719.htm
	Patch Vendor Advisory www.hustlelabs.com application/pdf Inactive Link Not Archived	 MISC www.hustlelabs.com/novell_ndps_advisory.pdf

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	4.83	sp3	All	All
Application	Novell	Client	4.90	sp2	All	All
Application	Novell	Client	4.91	sp2	All	All
Application	Novell	Client	4.83	sp3	All	All
Application	Novell	Client	4.90	sp2	All	All
Application	Novell	Client	4.91	sp2	All	All
cpe:2.3:a:novell:client:4.83:sp3:*****:						
cpe:2.3:a:novell:client:4.90:sp2:*****:						
cpe:2.3:a:novell:client:4.91:sp2:*****:						
cpe:2.3:a:novell:client:4.83:sp3:*****:						
cpe:2.3:a:novell:client:4.90:sp2:*****:						
cpe:2.3:a:novell:client:4.91:sp2:*****:						

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](#)