



CVE-2003-1591

Published on: 04/05/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:44 PM UTC

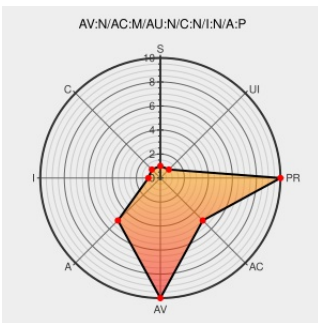
CVE-2003-1591

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of **Netware** from **Novell** contain the following vulnerability:

NWFTPD.nlm in the FTP server in Novell NetWare 6.0 before SP4 and 6.5 before SP1 allows user-assisted remote attackers to cause a denial of service (console hang) via a large number of FTP sessions, which are not properly handled during an NLM unload.

CVE-2003-1591 has been assigned by [M cve@mitre.org](mailto:cve@mitre.org) to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
What fixes are in NWFTPD.NLM v5.10.01, March 26, 2010?	www.novell.com text/html	ot CONFIRM www.novell.com/support/viewContent.do?externalId=3238588&sliceId=1

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
------	--------	---------	---------	--------	---------	----------

Operating System	Novell	Netware	6.0	All	All	All
Operating System	Novell	Netware	6.0	sp1	All	All
Operating System	Novell	Netware	6.0	sp2	All	All
Operating System	Novell	Netware	6.0	sp3	All	All
Operating System	Novell	Netware	6.5	All	All	All
Operating System	Novell	Netware	6.0	All	All	All
Operating System	Novell	Netware	6.0	sp1	All	All
Operating System	Novell	Netware	6.0	sp2	All	All
Operating System	Novell	Netware	6.0	sp3	All	All
Operating System	Novell	Netware	6.5	All	All	All
cpe:2.3:o:novell:netware:6.0:*:*:*:*:*:						
cpe:2.3:o:novell:netware:6.0:sp1:*:*:*:*:*:						
cpe:2.3:o:novell:netware:6.0:sp2:*:*:*:*:*:						
cpe:2.3:o:novell:netware:6.0:sp3:*:*:*:*:*:						
cpe:2.3:o:novell:netware:6.5:*:*:*:*:*:						
cpe:2.3:o:novell:netware:6.0:*:*:*:*:*:						
cpe:2.3:o:novell:netware:6.0:sp1:*:*:*:*:*:						
cpe:2.3:o:novell:netware:6.0:sp2:*:*:*:*:*:						
cpe:2.3:o:novell:netware:6.0:sp3:*:*:*:*:*:						
cpe:2.3:o:novell:netware:6.5:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)