



CVE-2002-1417

Published on: 04/11/2003 04:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:01 PM UTC

CVE-2002-1417

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

Directory traversal vulnerability in Novell NetBasic Scripting Server (NSN) for Netware 5.1 and 6, and Novell Small Business Suite 5.1 and 6, allows remote attackers to read arbitrary files via a URL containing a "..%5c" sequence (modified dot-dot), which is mapped to the directory separator.

CVE-2002-1417 has been assigned by [M cve@mitre.org](mailto:cve@mitre.org) to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access Vector

Access Complexity

Authentication

NETWORK

LOW

NONE

Confidentiality Impact

Integrity Impact

Availability Impact

PARTIAL

NONE

NONE

CVE References

Description

Tags

Link

Neohapsis Archives - Bugtraq - NOVL-2002-2963297 - NetBasic Buffer Overflow + Scripting Vulnerability - From ereed_at_novell.com

Patch

Vendor Advisory

web.archive.org

text/html

Inactive Link

Not Archived

[BUGTRAQ 20020820 NOVL-2002-2963297 - NetBasic Buffer Overflow + Scripting Vulnerability](#)

ISS X-Force Database: novell-netbasic-directory-traversal (9910): Novell NetBasic Scripting Handler (NSN) URL encoded backslash directory traversal

Patch

Vendor Advisory

web.archive.org

text/html

Inactive Link

Not Archived

[XF novell-netbasic-directory-traversal\(9910\)](#)

Novell Technical Information Document

support.novell.com

text/html

[CONFIRM](#)

support.novell.com/servlet/tidfinder/2963297

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	5.1	All	All	All
Operating System	Novell	Netware	6.0	All	All	All
Operating System	Novell	Netware	5.1	All	All	All
Operating System	Novell	Netware	6.0	All	All	All
Application	Novell	Small Business Suite	5.1	All	All	All
Application	Novell	Small Business Suite	6.0	All	All	All
Application	Novell	Small Business Suite	5.1	All	All	All
Application	Novell	Small Business Suite	6.0	All	All	All
cpe:2.3:o:novell:netware:5.1:*:*:*:*:*:						
cpe:2.3:o:novell:netware:6.0:*:*:*:*:*:						
cpe:2.3:o:novell:netware:5.1:*:*:*:*:*:						
cpe:2.3:o:novell:netware:6.0:*:*:*:*:*:						
cpe:2.3:a:novell:small_business_suite:5.1:*:*:*:*:*:						
cpe:2.3:a:novell:small_business_suite:6.0:*:*:*:*:*:						
cpe:2.3:a:novell:small_business_suite:5.1:*:*:*:*:*:						
cpe:2.3:a:novell:small_business_suite:6.0:*:*:*:*:*:						

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](#)