

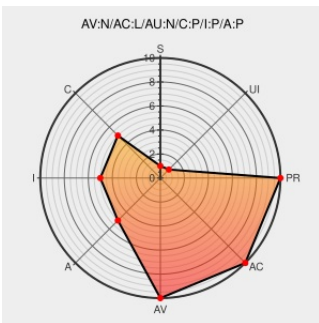


CVE-2005-4197

Published on: 12/13/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:21 PM UTC

CVE-2005-4197

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

Certain versions of [Ssl Vpn](#) from [Nortel](#) contain the following vulnerability:

tunnelform.yaws in Nortel SSL VPN 4.2.1.6 allows remote attackers to execute arbitrary commands via a link in the a parameter, which is executed with extra privileges in a cryptographically signed Java Applet.

CVE-2005-4197 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

Nortel SSL VPN Web Interface Input Validation Vulnerability

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

[🌐 BID 15798](#)

404 - Page not found! - SEC Consult

[Exploit](#)
[web.archive.org](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

★ [MISC www.sec-consult.com/247.html](#)

SecurityTracker.com Archives - Nortel SSL VPN Input Validation Flaw Lets Remote Users Conduct Cross-Site Scripting and Command Execution Attacks

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

[🌐 SECTrack 1015341](#)

Secunia - Advisories - Nortel SSL VPN Web Interface Arbitrary Command Execution Vulnerability

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

[X](#) [SECUNIA 17974](#)

SecurityFocus

www.securityfocus.com
text/html

 **BUGTRAQ 20051212 SEC**
Consult SA-20051211-0 :: Nortel SSL VPN Cross Site Scripting/Command Execution

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

www.vupen.com
text/html

 **VUPEN ADV-2005-2845**

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	Nortel	Ssl Vpn	4.1.2.11	All	All	All
Application	Nortel	Ssl Vpn	4.1.2.12	All	All	All
Application	Nortel	Ssl Vpn	4.1.2.11	All	All	All
Application	Nortel	Ssl Vpn	4.1.2.12	All	All	All
Application	Nortel	Ssl Vpn	All	All	All	All

cpe:2.3:a:nortel:ssl_vpn:4.1.2.11:*****:

cpe:2.3:a:nortel:ssl_vpn:4.1.2.12:*****:

cpe:2.3:a:nortel:ssl_vpn:4.1.2.11:*****:

cpe:2.3:a:nortel:ssl_vpn:4.1.2.12:*****:

cpe:2.3:a:nortel:ssl_vpn:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)