



CVE-2004-2549

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:13 PM UTC

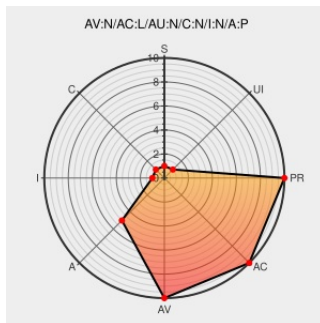
CVE-2004-2549

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Wlan Access Point 2220](#) from [Nortel](#) contain the following vulnerability:

Nortel Wireless LAN (WLAN) Access Point (AP) 2220, 2221, and 2225 allow remote attackers to cause a denial of service (service crash) via a TCP request with a large string, followed by 8 newline characters, to (1) the Telnet service on TCP port 23 and (2) the HTTP service on TCP port 80, possibly due to a buffer overflow.

CVE-2004-2549 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

No Description Provided

www.osvdb.org

OSVDB 4128

Inactive Link Not Archived

Nortel Wireless LAN Access Point 2200 Admin Port Can Be Crashed By Remote Users - SecurityTracker

securitytracker.com
text/html

SECTrack 1009294

IBM X-Force Exchange

exchange.xforce.ibmcloud.com
text/html

XF nortel-accesspoint-telnet-dos(15373)

No Description Provided

www116.nortelnetworks.com

MISC
www116.nortelnetworks.com/docs/bvdoc/wlan/216109a.pdf

Inactive Link Not Archived

No Description Provided

web.archive.org

text/html

Inactive Link

Not Archived

FULLDISC 20040301 Nortel Networks Wireless LAN Access Point 2200 DoS + PoC

Nortel Wireless LAN Access Point 2200 Series Denial Of Service Vulnerability

Exploit

cve.report (archive)

text/html

BID 9787

Secunia - Advisories - Nortel WLAN Access Point 2200 Denial of Service

Vendor Advisory

web.archive.org

text/html

SECUNIA 11034

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

Exploit/POC from Github

Nortel Wireless LAN Access Point 2200 Series - Denial of Service

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Nortel	Wlan Access Point 2220	All	All	All	All
Hardware 	Nortel	Wlan Access Point 2220	All	All	All	All
Hardware 	Nortel	Wlan Access Point 2221	All	All	All	All
Hardware 	Nortel	Wlan Access Point 2221	All	All	All	All
Hardware 	Nortel	Wlan Access Point 2225	All	All	All	All
Hardware 	Nortel	Wlan Access Point 2225	All	All	All	All
cpe:2.3:h:nortel:wlan_access_point_2220:*****:						
cpe:2.3:h:nortel:wlan_access_point_2220:*****:						
cpe:2.3:h:nortel:wlan_access_point_2221:*****:						
cpe:2.3:h:nortel:wlan_access_point_2221:*****:						
cpe:2.3:h:nortel:wlan_access_point_2225:*****:						
cpe:2.3:h:nortel:wlan_access_point_2225:*****:						

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](#)