



CVE-2002-2300

Published on: 12/31/2002 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:05 PM UTC

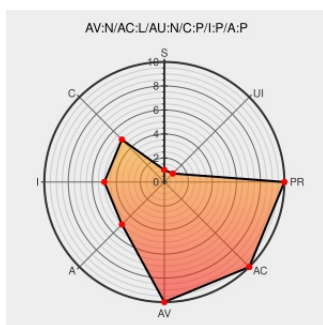
CVE-2002-2300

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Webbngss3nbxnts](#) from [3com](#) contain the following vulnerability:

Buffer overflow in ftpd 5.4 in 3Com NBX 4.0.17 or ftpd 5.4.2 in 3Com NBX 4.1.4 allows remote attackers to cause a denial of service (crash) via a long CEL command.

CVE-2002-2300 has been assigned by [M](#) [cve@mitre.org](#) to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

Access
Complexity

Authentication

NETWORK

LOW

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

PARTIAL

PARTIAL

PARTIAL

CVE References

Description

Tags

Link

Bugtraq: 3com NBX IP Phone Call manager Denial of Service - Update

[seclists.org](#)
[text/html](#)

[BUGTRAQ 20030427 3com NBX IP Phone Call manager Denial of Service - Update](#)

3Com SuperStack 3 NBX FTPD Denial of Service Vulnerability

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

[BID 6297](#)

CERT Vulnerability Notes Database

[US Government Resource](#)
[www.kb.cert.org](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[CERT-VN VU#317417](#)

3com NBX IP phone system Denial of Service Attack - SECNAP First Alert

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

[MISC](#)
[www.secnap.com/alerts.php?pg=6](#)

404 Not Found - SecurityTracker - Page Not Found	securitytracker.com text/html	 SECTrack 1006760
3Com SuperStack 3 NBX and NBX 100 Telephony Systems Can Be Crashed By Remote Users Sending FTP Commands - SecurityTracker	securitytracker.com text/html	 SECTrack 1005732
No Description Provided	marc.info text/html	 BUGTRAQ 20021202 [VU#317417] Denial of Service condition in vxworks ftpd/3com nbx
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF 3com-nbx-cel-bo(10739)

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
Hardware  	3com	Webbngss3nbxnts	4.0.17	All	All	All
Hardware  	3com	Webbngss3nbxnts	4.1.21	All	All	All
Hardware  	3com	Webbngss3nbxnts	4.1.4	All	All	All
Hardware  	3com	Webbngss3nbxnts	4.0.17	All	All	All
Hardware  	3com	Webbngss3nbxnts	4.1.21	All	All	All
Hardware  	3com	Webbngss3nbxnts	4.1.4	All	All	All
cpe:2.3:h:3com:webbngss3nbxnts:4.0.17:*****:						
cpe:2.3:h:3com:webbngss3nbxnts:4.1.21:*****:						
cpe:2.3:h:3com:webbngss3nbxnts:4.1.4:*****:						
cpe:2.3:h:3com:webbngss3nbxnts:4.0.17:*****:						
cpe:2.3:h:3com:webbngss3nbxnts:4.1.21:*****:						
cpe:2.3:h:3com:webbngss3nbxnts:4.1.4:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)