

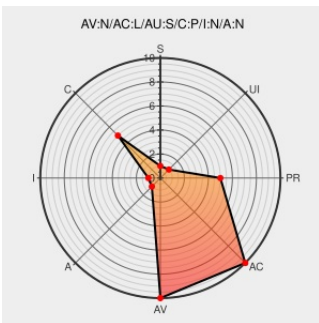


CVE-2004-2488

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

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

CVE-2004-2488

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

Certain versions of [Nexgen Ftp Server](#) from [Nexgen](#) contain the following vulnerability:

Directory traversal vulnerability in Nexgen FTP Server before 2.2.3.23 allows remote authenticated users to read or list arbitrary files via "C:" sequences in the (1) RETR (get), (2) NLST (ls), (3) LIST (ls), (4) RNFR, or (5) RNTD FTP commands.

CVE-2004-2488 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

SINGLE

Confidentiality
Impact

PARTIAL

Integrity
Impact

NONE

Availability
Impact

NONE

CVE References

Description

Tags

Link

HugeDomains.com - NexGenServer.com is for sale (Nex Gen Server)

www.nexgenserver.com
[text/html](#)

[CONFIRM](#)
www.nexgenserver.com/cgi-bin/loadframe2.cgi?/History.html

Secunia - Advisories - Nexgen FTP Server Directory Traversal Vulnerability

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

[SECUNIA 11216](#)

SecurityTracker.com Archives - Nextgen FTP Server Discloses Arbitrary Files to Remote Authenticated Users

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

[SECTRAK 1009545](#)

No Description Provided

[Exploit](#)
www.osvdb.org

[OSVDB 4557](#)

Inactive Link **Not Archived**

IBM X-Force Exchange

exchange.xforce.ibmcloud.com

text/html

XF nexgen-dotdot-directory-traversal(15594)

NexGen FTP Server Remote Directory Traversal Vulnerability

Patch

cve.report (archive)

text/html

BID 9970

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	Nexgen	Nexgen Ftp Server	1.0	All	All	All
Application	Nexgen	Nexgen Ftp Server	2.0	All	All	All
Application	Nexgen	Nexgen Ftp Server	2.1	All	All	All
Application	Nexgen	Nexgen Ftp Server	2.2	All	All	All
Application	Nexgen	Nexgen Ftp Server	1.0	All	All	All
Application	Nexgen	Nexgen Ftp Server	2.0	All	All	All
Application	Nexgen	Nexgen Ftp Server	2.1	All	All	All
Application	Nexgen	Nexgen Ftp Server	2.2	All	All	All
cpe:2.3:a:nexgen:nexgen_ftp_server:1.0:*.~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:a:nexgen:nexgen_ftp_server:2.0:*.~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:a:nexgen:nexgen_ftp_server:2.1:*.~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:a:nexgen:nexgen_ftp_server:2.2:*.~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:a:nexgen:nexgen_ftp_server:1.0:*.~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:a:nexgen:nexgen_ftp_server:2.0:*.~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:a:nexgen:nexgen_ftp_server:2.1:*.~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:a:nexgen:nexgen_ftp_server:2.2:*.~::~~::~~::~~::~~::~~::~~::						

No vendor comments have been submitted for this CVE

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](#)