



CVE-2004-2253

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

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

CVE-2004-2253

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Surgeldap](#) from [Netwin](#) contain the following vulnerability:

Directory traversal vulnerability in user.cgi in SurgeLDAP 1.0g and earlier allows remote attackers to read arbitrary files via a `..` in the page parameter of the show command.

CVE-2004-2253 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

PARTIAL

Integrity
Impact

NONE

Availability
Impact

NONE

CVE References

Description

Tags

Link

Page not found - CVE.report

[Exploit](#)
[Vendor Advisory](#)
[members.lycos.co.uk](#)
[text/plain](#)
[Inactive Link](#) [Not Archived](#)

[MISC](#)
members.lycos.co.uk/r34ct/main/SurgeLDAP%201.0g.txt

Secunia - Advisories - SurgeLDAP Arbitrary File Retrieval Vulnerability

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

[SECUNIA 11343](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

[XF surgeldap-dotdot-directory-traversal\(15851\)](#)

SurgeLDAP User.CGI Directory Traversal Vulnerability

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

[BID 10103](#)

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	Netwin	Surgeldap	1.0d	All	All	All
Application	Netwin	Surgeldap	1.0e	All	All	All
Application	Netwin	Surgeldap	1.0g	All	All	All
Application	Netwin	Surgeldap	1.0d	All	All	All
Application	Netwin	Surgeldap	1.0e	All	All	All
Application	Netwin	Surgeldap	1.0g	All	All	All
cpe:2.3:a:netwin:surgeldap:1.0d:*****:						
cpe:2.3:a:netwin:surgeldap:1.0e:*****:						
cpe:2.3:a:netwin:surgeldap:1.0g:*****:						
cpe:2.3:a:netwin:surgeldap:1.0d:*****:						
cpe:2.3:a:netwin:surgeldap:1.0e:*****:						
cpe:2.3:a:netwin:surgeldap:1.0g:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)