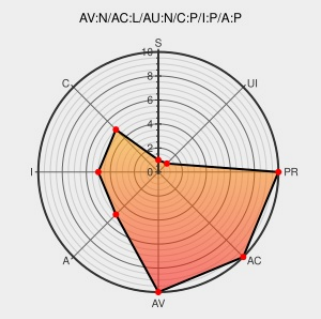
CVE-2004-2271

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

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

CVE-2004-2271

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Minimal Http Server from Minishare contain the following vulnerability:

Buffer overflow in MiniShare 1.4.1 and earlier allows remote attackers to execute arbitrary code via a long HTTP GET request.

CVE-2004-2271 has been assigned by 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
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF minishare-address-link-bo(17978)
MiniShare Server Remote Buffer Overflow Vulnerability	Exploit cve.report (archive) text/html	BID 11620
Secunia - Advisories - MiniShare HTTP "GET" Request Buffer Overflow Vulnerability	Patch Vendor Advisory web.archive.org text/html	SECUNIA 13114
'MiniShare Remote Buffer Overflow' - SecuriTeam	Exploit www.securiteam.com text/x-c	MISC www.securiteam.com/exploits/6X00B1PBPC.html
Neohapsis Archives - Full Disclosure List - #0208 - [Full-	Vendor Advisory	FULLDISC 20041107 [New VULNERABILTY

Disclosure] [New VULNERABILTY + Exploit] MiniShare, Minimal HTTP Server for Windows, Remote Buffer Overflow Exploit	web.archive.org text/html Inactive Link Not Archived	+ Exploit] MiniShare, Minimal HTTP Server for Windows, Remote Buffer Overflow Exploit
SecurityTracker.com Archives - MiniShare Buffer Overlow in Processing Long URLs Lets Remote Users Execute Arbitrary Code	Exploit securitytracker.com text/html	SECTRACK 1012106
SourceForge.net: File Release Notes and Changelog	Patch web.archive.org text/html Inactive Link Not Archived	CONFIRM sourceforge.net/project/shownotes.php?release_id=241158
No Description Provided	Patch www.osvdb.org Inactive Link Not Archived	OSVDB 11530

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

Minishare 1.4.1 Remote Buffer Overflow

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Minishare	Minimal Http Server	All	All	All	All

cpe:2.3:a:minishare:minimal_http_server:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→