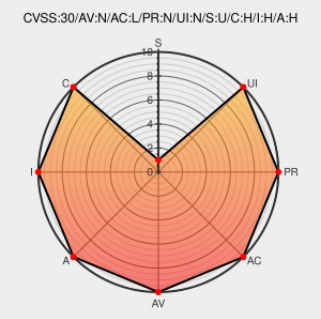
CVE-2018-19861

Published on: 01/03/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:40 PM UTC

CVE-2018-19861

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



Certain versions of Minishare from Minishare Project contain the following vulnerability:

Buffer overflow in MiniShare 1.4.1 and earlier allows remote attackers to execute arbitrary code via a long HTTP HEAD request. NOTE: this product is discontinued.

CVE-2018-19861 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

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
MiniShare 1.4.1 HEAD / POST Buffer Overflow ≈ Packet Storm	Exploit Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/150689/MiniShare-1.4.1-HEAD-POST-Buffer-Overflow.html

Full Disclosure: [CVE-2018-19861, CVE-2018-19862] Buffer overflow in MiniShare 1.4.1 HEAD and POST method	Exploit Mailing List Third Party Advisory seclists.org text/html	FULLDISC 20181207 [CVE-2018-19861, CVE-2018-19862] Buffer overflow in MiniShare 1.4.1 HEAD and POST method
MiniShare 1.4.1 - 'HEAD/POST' Remote Buffer Overflow - Windows remote Exploit	Exploit Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 45999

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	Minishare Project	Minishare	All	All	All	All

cpe:2.3:a:minishare_project:minishare:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→