

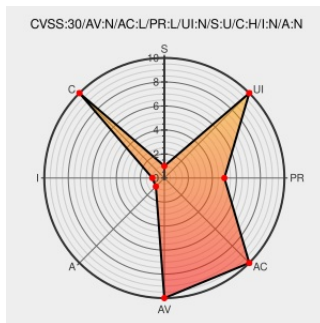


CVE-2017-9382

Published on: 06/17/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:56 PM UTC

CVE-2017-9382

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

Certain versions of [Veraedge](#) from [Getvera](#) contain the following vulnerability:

An issue was discovered on Vera VeraEdge 1.7.19 and Veralite 1.7.481 devices. The device provides UPnP services that are available on port 3480 and can also be accessed via port 80 using the url "/port_3480". It seems that the UPnP services provide "file" as one of the service actions for a normal user to read a file that is stored under

the /etc/cmh-lu folder. It retrieves the value from the "parameters" query string variable and then passes it to an internal function "FileUtils::ReadFileIntoBuffer" which is a library function that does not perform any sanitization on the value submitted and this allows an attacker to use directory traversal characters "../" and read files from other folders within the device.

CVE-2017-9382 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **4 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Veralite / Veraedge Router XSS / Command Injection / CSRF / Traversal ≈ Packet Storm	Third Party Advisory VDB Entry packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/153242/Veralite-Veraedge-Router-XSS-Command-Injection-CSRF-Traversal.html
IoT_vulnerabilities/Vera_sec_issues.pdf at master · ethanhunnt/IoT_vulnerabilities · GitHub	Exploit Third Party Advisory github.com text/html	 MISC github.com/ethanhunnt/IoT_vulnerabilities/blob/master/Vera_sec_issues.pdf
Bugtraq: Newly releases IoT security issues	Mailing List Third Party Advisory seclists.org text/html	 BUGTRAQ 20190609 Newly releases IoT security issues

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 	Getvera	Veraedge	-	All	All	All
Hardware 	Getvera	Veraedge	-	All	All	All
Operating System	Getvera	Veraedge Firmware	All	All	All	All
Hardware 	Getvera	Veralite	-	All	All	All
Hardware 	Getvera	Veralite	-	All	All	All
Operating System	Getvera	Veralite Firmware	All	All	All	All
cpe:2.3:h:getvera:veraedge:-:*:*:*:*:*:						
cpe:2.3:h:getvera:veraedge:-:*:*:*:*:*:						
cpe:2.3:o:getvera:veraedge_firmware:*:*:*:*:*:						
cpe:2.3:h:getvera:veralite:-:*:*:*:*:*:						
cpe:2.3:h:getvera:veralite:-:*:*:*:*:*:						
cpe:2.3:o:getvera:veralite_firmware:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

© [CVE.report](#) 2023  |

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](#)