

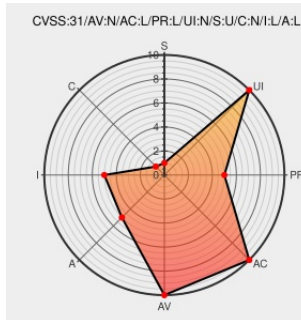


CVE-2019-17656

Published on: 04/12/2021 12:00:00 AM UTC

Last Modified on: 04/19/2021 04:24:00 PM UTC

CVE-2019-17656

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

Certain versions of [Fortios](#) from [Fortinet](#) contain the following vulnerability:

A Stack-based Buffer Overflow vulnerability in the HTTPD daemon of FortiOS 6.0.10 and below, 6.2.2 and below and FortiProxy 1.0.x, 1.1.x, 1.2.9 and below, 2.0.0 and below may allow an authenticated remote attacker to crash the service by sending a malformed PUT request to the server. Fortinet is not aware of any successful exploitation of this vulnerability that would lead to code execution.

CVE-2019-17656 has been assigned by psirt@fortinet.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Fortinet - Fortinet FortiProxy, FortiOS version FortiProxy 1.0.x, 1.1.x, 1.2.9 and below, 2.0.0 and below; FortiOS 6.0.10 and below, 6.2.2 and below**

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	NONE	NONE	HIGH

CVSS2 Score: **4 - MEDIUM**

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

CVE References

Description	Tags	Link
-------------	------	------

Description	Tags	Link
FortiOS HTTPD is vulnerable to a Stack-based Buffer Overflow vulnerability FortiGuard	fortiguard.com text/html	 CONFIRM fortiguard.com/advisory/FG-IR-19-248
FortiProxy - HTTPD is vulnerable to a Stack-based Buffer Overflow vulnerability FortiGuard	fortiguard.com text/html	 CONFIRM fortiguard.com/advisory/FG-IR-21-007

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.

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fortinet	Fortios	All	All	All	All
Operating System	Fortinet	Fortios	All	All	All	All
Application	Fortinet	Fortiproxy	All	All	All	All
cpe:2.3:o:fortinet:fortios:*.*.*.*.*.*.*.*:						
cpe:2.3:o:fortinet:fortios:*.*.*.*.*.*.*.*:						
cpe:2.3:a:fortinet:fortiproxy:*.*.*.*.*.*.*.*:						

Social Mentions		
Source	Title	Posted (UTC)
 @autumn_good_35	CVE-2019-17656 FortiProxy - HTTPD is vulnerable to a Stack-based Buffer Overflow vulnerability fortiguard.com/psirt/FG-IR-21...	2021-04-07 15:01:54
 @CVEreport	CVE-2019-17656 : A Stack-based Buffer Overflow vulnerability in the HTTPD daemon of FortiOS 6.0.10 and below, 6.2.... twitter.com/i/web/status/1...	2021-04-12 14:31:05
 /r/netcve	CVE-2019-17656	2021-04-12 14:40:11

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](#)