



CVE-2019-15703

Published on: 10/24/2019 12:00:00 AM UTC

Last Modified on: 03/31/2022 05:53:00 PM UTC

CVE-2019-15703

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

An Insufficient Entropy in PRNG vulnerability in Fortinet FortiOS 6.2.1, 6.2.0, 6.0.8 and below for device not enable hardware TRNG token and models not support builtin TRNG seed allows attacker to theoretically recover the long term ECDSA secret in a TLS client with a RSA handshake and mutual ECDSA authentication via the help of flush+reload side channel attacks in FortiGate VM models only.

CVE-2019-15703 has been assigned by psirt@fortinet.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Fortinet** - **Fortinet FortiOS** version **6.2.1**

Affected Vendor/Software: **Fortinet** - **Fortinet FortiOS** version **6.2.0**

Affected Vendor/Software: **Fortinet** - **Fortinet FortiOS** version **6.0.8 and below**

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **2.6 - LOW**

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
FortiOS DRBG insufficient entropy FortiGuard	Vendor Advisory fortiguard.com text/html	 MISC fortiguard.com/psirt/FG-IR-19-186

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.

44081 FortiOS DRBG insufficient entropy (FG-IR-19-186)

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
Operating System	Fortinet	Fortios	All	All	All	All
cpe:2.3:o:fortinet:fortios:*.*.*.*.*.*.*.*.						
cpe:2.3:o:fortinet:fortios:*.*.*.*.*.*.*.*.						
cpe:2.3:o:fortinet:fortios:*.*.*.*.*.*.*.*.						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© 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