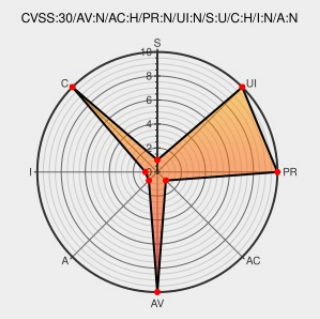
CVE-2018-9194

Published on: 09/05/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:55 PM UTC

CVE-2018-9194

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



Certain versions of Fortios from Fortinet contain the following vulnerability:

A plaintext recovery of encrypted messages or a Man-in-the-middle (MiTM) attack on RSA PKCS #1 v1.5 encryption may be possible without knowledge of the server's private key. Fortinet FortiOS 5.4.6 to 5.4.9, 6.0.0 and 6.0.1 are vulnerable by such attack under VIP SSL feature when CPx being used.

CVE-2018-9194 has been assigned by psirt@fortinet.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Fortinet, Inc.** - **FortiOS** version **6.0.1, 6.0.0**

Affected Vendor/Software: **Fortinet, Inc.** - **FortiOS** version **5.4.9, 5.4.8, 5.4.7, 5.4.6**

CVSS3 Score: 5.9 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link

The ROBOT Attack - Return of Bleichenbacher's Oracle Threat | FortiGuard	Vendor Advisory fortiguard.com text/html	CONFIRM fortiguard.com/advisory/FG-IR-17-302
The ROBOT Attack - Return of Bleichenbacher's Oracle Threat	Third Party Advisory robotattack.org text/html	MISC robotattack.org/
VU#144389 - TLS implementations may disclose side channel information via discrepancies between valid and invalid PKCS#1 padding	Third Party Advisory US Government Resource www.kb.cert.org text/html	CERT-VN VU#144389

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
Operating System	Fortinet	Fortios	6.0.0	All	All	All
Operating System	Fortinet	Fortios	6.0.1	All	All	All
Operating System	Fortinet	Fortios	6.0.0	All	All	All
Operating System	Fortinet	Fortios	6.0.1	All	All	All
Operating System	Fortinet	Fortios	All	All	All	All

cpe:2.3:o:fortinet:fortios:6.0.0:*:*:*:*:*:*:*:

cpe:2.3:o:fortinet:fortios:6.0.1:*:*:*:*:*:*:*:

cpe:2.3:o:fortinet:fortios:6.0.0:*:*:*:*:*:*:*:

cpe:2.3:o:fortinet:fortios:6.0.1:*:*:*:*:*:*:*:

cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report