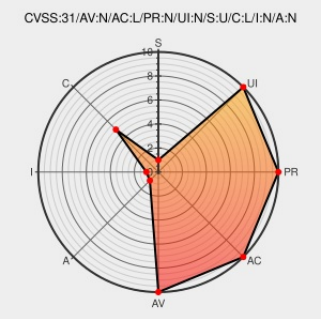
CVE-2020-6648

Published on: 10/21/2020 12:00:00 AM UTC

Last Modified on: 06/15/2022 03:18:00 AM UTC

CVE-2020-6648

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



Certain versions of Fortios from Fortinet contain the following vulnerability:

A cleartext storage of sensitive information vulnerability in FortiOS command line interface in versions 6.2.4 and earlier and FortiProxy 2.0.0, 1.2.9 and earlier may allow an authenticated attacker to obtain sensitive information such as users passwords by connecting to FortiGate CLI and executing the "diag sys ha checksum show" command.

CVE-2020-6648 has been assigned by psirt@fortinet.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Fortinet** - **FortiGate and FortiProxy** version **FortiOS versions 6.2.4 and earlier and FortiProxy 2.0.0, 1.2.9 and earlier.**

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

Description	Tags	Link
FortiGuard	www.fortiguard.com text/html	CONFIRM www.fortiguard.com/psirt/FG-IR-20-236
Potential sensitive information can be displayed in cleartext in FortiOS CLI window | FortiGuard	Broken Link www.fortiguard.com text/html	CONFIRM www.fortiguard.com/psirt/FG-IR-20-009

Related QID Numbers

44078 FortiOS - Information Disclosure Vulnerability (FG-IR-20-009)

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
Application	Fortinet	Fortiproxy	2.0.0	All	All	All

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

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

cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*:*:*:

cpe:2.3:a:fortinet:fortiproxy:2.0.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@RemotelyAlerts	Severity: ?? | A cleartext storage of sensitive informa... | CVE-2020-6648 | Link for more: alerts.remotelyrmm.com/CVE-2020-6648	2022-06-15 04:31:25

← Previous ID

Next ID→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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