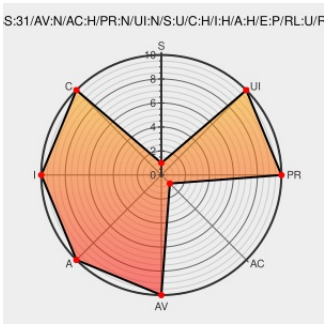
CVE-2021-26109

Published on: 12/08/2021 12:00:00 AM UTC

Last Modified on: 12/09/2021 08:52:00 PM UTC

CVE-2021-26109

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



Certain versions of Fortios from Fortinet contain the following vulnerability:

An integer overflow or wraparound vulnerability in the memory allocator of SSLVPN in FortiOS before 7.0.1 may allow an unauthenticated attacker to corrupt control data on the heap via specifically crafted requests to SSLVPN, resulting in potentially arbitrary code execution.

CVE-2021-26109 has been assigned by psirt@fortinet.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **Fortinet** - **Fortinet FortiOS** version **FortiOS before 7.0.1**

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
PSIRT Advisories | FortiGuard	fortiguard.com text/html	CONFIRM fortiguard.com/advisory/FG-IR-21-049

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.

Related QID Numbers

43915 FortiOS Integer Overflow Vulnerability in Secure Sockets Layer (SSL) Virtual Private Network (VPN) (SSLVPN) Allocator (FG-IR-21-049)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fortinet	Fortios	7.0.0	All	All	All
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:7.0.0:*:*:*:*:*:*:*:

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

Social Mentions

Source	Title	Posted (UTC)
@softek_jp	Fortinet FortiOS の SSLVPN アロケータの処理に任意のコードを実行される問題 (CVE-2021-26109) [40722] sid.softek.jp/content/show/4… #SIDfm #脆弱性情報	2021-12-08 07:32:31
@CVEreport	CVE-2021-26109 : An integer overflow or wraparound vulnerability in the memory allocator of SSLVPN in FortiOS befor… twitter.com/i/web/status/1…	2021-12-08 12:28:45
/r/netcve	CVE-2021-26109	2021-12-08 13:38:09

← 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