KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Critical Unauthenticated RCE Exploited in FortiOS SSL-VPN

Tracker ID: TN1213 **Date:** December 15, 2022 **Category:** Vulnerability **Industry:** All **Region**: All

Background

Fortinet has published a security advisory on a FortiOS vulnerability that might allow an attacker to perform unauthorized actions on vulnerable systems. CVE-2022-42475 (CVSS score: 9.3), FortiOS: heap-based buffer overflow in "sslvpnd" is a critical issue relating to a heap-based buffer overflow vulnerability [CWE-122] in FortiOS SSL-VPN that may allow a remote, unauthenticated attacker to execute arbitrary code or commands through specially crafted requests.

Fortinet's own operating system, FortiOS, is used across several product lines. An attacker could exploit this vulnerability to install programs, read, alter, or remove data, or create new accounts with full user rights, depending on the privileges connected with the user. Observing the exploitation attempts, it is recommended to immediately apply the patches or workarounds to disable the VPN-SSL functionality and create access rules to limit connections from specific IP addresses.

Detections

We have observed an exploit of this vulnerability in the wild and recommend that you validate your systems promptly against the below indicators of compromise:

Multiple log entries with:

- Logdesc="Application crashed" and msg="[...] application:sslvpnd,[...], Signal 11 received, Backtrace: [...]“

Presence of the following artifacts in the filesystem:

- /data/lib/libips.bak
- /data/lib/libgif.so
- /data/lib/libiptcp.so
- /data/lib/libipudp.so
- /data/lib/libjepg.so
- /var/.sslvpnconfigbk
- /data/etc/wxd.conf
- /flash

Connections to suspicious IP addresses from the FortiGate:

- 188.34.130.40:444
- 103.131.189.143:30080,30081,30443,20443
- 192.36.119.61:8443,444
- 172.247.168.153:8033

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Critical Unauthenticated RCE Exploited in FortiOS SSL-VPN

Tracker ID: TN1213 **Date:** December 15, 2022 **Category:** Vulnerability **Industry:** All **Region**: All

Analysis

CVE ID	Severity	CVSS Score
CVE-2022-42475	Critical	9.3

Affected Products and Versions

- FortiOS version 7.2.0 through 7.2.2
- FortiOS version 7.0.0 through 7.0.8
- FortiOS version 6.4.0 through 6.4.10
- FortiOS version 6.2.0 through 6.2.11
- FortiOS version 6.0.0 through 6.0.15
- FortiOS version 5.6.0 through 5.6.14
- FortiOS version 5.4.0 through 5.4.13
- FortiOS version 5.2.0 through 5.2.15
- FortiOS version 5.0.0 through 5.0.14
- FortiOS-6K7K version 7.0.0 through 7.0.7
- FortiOS-6K7K version 6.4.0 through 6.4.9
- FortiOS-6K7K version 6.2.0 through 6.2.11
- FortiOS-6K7K version 6.0.0 through 6.0.14

Recommendations

- Fortinet has released the security patches. Update to below:
  - FortiOS version 7.0.9 or above
  - FortiOS version 6.4.11 or above
  - FortiOS version 6.2.12 or above
  - Upcoming FortiOS version 6.0.16 or above
  - Upcoming FortiOS-6K7K version 7.0.8 or above
  - FortiOS-6K7K version 6.4.10 or above
  - Upcoming FortiOS-6K7K version 6.2.12 or above
  - FortiOS-6K7K version 6.0.15 or above

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Critical Unauthenticated RCE Exploited in FortiOS SSL-VPN

Tracker ID: TN1213 **Date:** December 15, 2022 **Category:** Vulnerability **Industry:** All **Region**: All

- In case the patches are delayed, Disable SSL-VPN as a workaround.
- Monitor the services and critical assets exposed to the Internet. Collect and review relevant logs, data and artifacts to identify any threat in the network.

References

- FortiGuard Labs, Fortinet, FortiOS - heap-based buffer overflow in sslvpnd, PSIRT Advisories, December 12, 2022, External Link (www.fortiguard.com).
- Lawrence Abrams, Fortinet says SSL-VPN pre-auth RCE bug is exploited in attacks, Bleeping Computer, December 12, 2022, External Link (www.bleepingcomputer.com).

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176471471

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia