Security Advisory 2022-086

Remote Code Execution Vulnerability in FortiOS SSL-VPN

December 13, 2022 — v1.0

TLP:CLEAR

History:

- *13/12/2022 — v1.0 – Initial publication*

Summary

On December 12, 2022, Fortinet released an advisory concerning a heap-based buffer overflow critical vulnerability in FortiOS SSL-VPN that could allow may allow a remote unauthenticated attacker to execute arbitrary code or commands via specifically crafted requests. This vulnerability CVE-2022-42475 has the CVSS score of 9.3.

Fortinet is aware of one instance where this vulnerability was exploited in the wild. They do not believe this to be trivial to exploit, however they are advising customers using SSL-VPN to upgrade immediately.

Technical Details

By exploiting this vulnerability `CVE-2022-42475` an attacker could manipulate the dynamic memory space of the process to such an extent that adjacent chunks may be corrupted to hijack its flow of execution.

Affected Products

The following products are affected [1]:

- 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-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

Upgrade to:

- FortiOS version 7.2.3 or above
- FortiOS version 7.0.9 or above
- FortiOS version 6.4.11 or above
- FortiOS version 6.2.12 or above
- FortiOS-6K7K version 7.0.8 or above
- FortiOS-6K7K version 6.4.10 or above
- FortiOS-6K7K version 6.2.12 or above
- FortiOS-6K7K version 6.0.15 or above

Check your systems if there are multiple log entries with:

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

Check the presence of the following artefacts 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`

Check for any 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`

Workaround:

Disable SSLVPN until the upgrade can be performed.

References

[1] https://www.fortiguard.com/psirt/FG-IR-22-398