A part of the **Department of the Environment, Climate & Communications**

NCSC Alert

Critical Vulnerability in Fortinet FortiOS sslvpnd (CVE-2022-42475)

Tuesday 13th December, 2022

STATUS: TLP-CLEAR

Description

A critical vulnerability has been discovered in Fortinet FortiOS sslvpnd which may allow an unauthenticated attacker to execute arbitrary code or commands via crafted requests. Fortinet is aware of an instance where this was exploited in the wild.

You can view the Fortinet advisory here: https://www.fortiguard.com/psirt/FG-IR-22-398. The CVE-2022-42475 vulnerability has been assigned a CVSSv3 score of 9.3 (critical).

Products Affected

- 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

Impact

Exploitation of CVE-2022-42475 could allow an attacker to remotely execute code and carry out data theft, operational disruption, ransomware and denial of service.

Detection

Fortinet recommends that affected organisations validate systems against the following 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

Recommendations

- FortiOS version 7.2.0 through 7.2.2

    – Upgrade to FortiOS version 7.2.3 or above

- FortiOS version 7.0.0 through 7.0.8

    – Upgrade to FortiOS version 7.0.9 or above

- FortiOS version 6.4.0 through 6.4.10

    – Upgrade to FortiOS version 6.4.11 or above

- FortiOS version 6.2.0 through 6.2.11

    – Upgrade to FortiOS version 6.2.12 or above

- FortiOS-6K7K version 7.0.0 through 7.0.7

    – Upgrade to FortiOS-6K7K version 7.0.8 or above

- FortiOS-6K7K version 6.4.0 through 6.4.9

    – Upgrade to FortiOS-6K7K version 6.4.10 or above

- FortiOS-6K7K version 6.2.0 through 6.2.11

    – Upgrade to FortiOS-6K7K version 6.2.12 or above

- FortiOS-6K7K version 6.0.0 through 6.0.14

    – Upgrade to FortiOS-6K7K version 6.0.15 or above

The NCSC also advises:

- Disable VPN-SSL functionality if it is not essential

- Examine logs to check that no unauthorised access has been attained

- Implement conditional access rules (such as GeoIP blocking) to limit your exposure vector

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie