TLP: Clear[1]

UPDATE: [14th June 2023]: A critical vulnerability in Fortinet Fortigate SSL-VPN devices.

Dear Constituents,

CERT Tonga is aware of a critical vulnerability which is a Remote Code Execution *(CVE-2023-27997)* has been identified in multiple versions of Fortinet Fortigate devices when SSL-VPN enabled.

How it works

Exploitation of this vulnerability could allow a malicious actor to gain remote code execution rights on the affected system and perform unauthorised actions.

FortiGate devices running SSL-VPN enabled are potentially at risk.

- FortiOS-6K7K version 7.0.10
- FortiOS-6K7K version 7.0.5
- FortiOS-6K7K version 6.4.12
- FortiOS-6K7K version 6.4.10
- FortiOS-6K7K version 6.4.8
- FortiOS-6K7K version 6.4.6
- FortiOS-6K7K version 6.4.2
- FortiOS-6K7K version 6.2.9 through 6.2.13
- FortiOS-6K7K version 6.2.6 through 6.2.7
- FortiOS-6K7K version 6.2.4
- FortiOS-6K7K version 6.0.12 through 6.0.16
- FortiOS-6K7K version 6.0.10
- FortiProxy version 7.2.0 through 7.2.3
- FortiProxy version 7.0.0 through 7.0.9

1 CERT Tonga adopts the Traffic Light Protocol

- FortiProxy version 2.0.0 through 2.0.12
- FortiProxy 1.2 all versions
- FortiProxy 1.1 all versions
- FortiOS version 7.2.0 through 7.2.4
- FortiOS version 7.0.0 through 7.0.11
- FortiOS version 6.4.0 through 6.4.12
- FortiOS version 6.0.0 through 6.0.16

What to do

To System administrators and users, due to the critical nature of this vulnerability, we highly recommend upgrading your devices running FortiOS and FortiProxy to the latest version.

- upgrade to FortiOS-6K7K version 7.0.12 or above
- upgrade to FortiOS-6K7K version 6.4.13 or above
- upgrade to FortiOS-6K7K version 6.2.15 or above
- upgrade to FortiOS-6K7K version 6.0.17 or above
- upgrade to FortiProxy version 7.2.4 or above
- upgrade to FortiProxy version 7.0.10 or above
- upgrade to FortiProxy version 2.0.13 or above
- upgrade to FortiOS version 7.4.0 or above
- upgrade to FortiOS version 7.2.5 or above
- upgrade to FortiOS version 7.0.12 or above
- upgrade to FortiOS version 6.4.13 or above
- upgrade to FortiOS version 6.2.14 or above
- upgrade to FortiOS version 6.0.17 or above

However, for alternative mitigation CERT Tonga recommends disabling SSL-VPN.

Reference

For further details you can also find it in the link provided.

- https://www.fortiguard.com/psirt
- https://www.fortinet.com/blog/psirt-blogs/analysis-of-cve-2023-27997-and-clarifications-on-volt-typhoon-campaign

For more information, please contact us:

CERT Tonga
Ministry of MEIDECC
Nuku'alofa
Tel: 2378 (CERT)
Email: cert@cert.gov.to
Web: www.cert.gov.to
Twitter: @CERTTonga | Facebook: @CERTTonga

Disclaimer Notice: