SamCERT Advisory

8th March 2023

Fortinet software Remote Code Execution and Denial of Service vulnerability.
A vulnerability has been discovered that affects FortiOS and FortiProxy's administrative interface. FortiOS is used on FortiGate, and FortiWifi devices.

This vulnerability (CVE-2023-25610) allows an attacker to run unauthorised commands remotely on some affected systems.

It also allows an attacker to remotely crash affected devices, making them unavailable.

What to look for and how to tell if you're at risk.

The vulnerable versions are:

- FortiOS version 7.2.0 through 7.2.3
- FortiOS version 7.0.0 through 7.0.9
- FortiOS version 6.4.0 through 6.4.11
- FortiOS version 6.2.0 through 6.2.12
- FortiOS 6.0 all versions
- FortiProxy version 7.2.0 through 7.2.2
- FortiProxy version 7.0.0 through 7.0.8
- FortiProxy version 2.0.0 through 2.0.11
- FortiProxy 1.2 all versions
- FortiProxy 1.1 all versions

Some devices running FortiOS are only vulnerable to the denial of service attack while others are vulnerable to both denial of service and remote code execution. *Check Fortinet's advisory for the latest information on which devices are only vulnerable to the denial of service.*

What to do to prevent it.

Upgrade your products to the latest version:
FortiOS version 7.4.0 or above
FortiOS version 7.2.4 or above
FortiOS version 7.0.10 or above
FortiOS version 6.4.12 or above
FortiOS version 6.2.13 or above
FortiProxy version 7.2.3 or above
FortiProxy version 7.0.9 or above
FortiProxy version 2.0.12 or above
FortiOS-6K7K version 7.0.10 or above
FortiOS-6K7K version 6.4.12 or above
FortiOS-6K7K version 6.2.13 or above

Mitigation
To mitigate this vulnerability, we advise that you disable the HTTP/HTTPS administrative interface or restrict access to only trusted networks or IP addresses.
For further mitigations, Fortinet has provided workarounds on their advisory.