UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0289

FORTINET PATCHES NEW RCE VULNERABILITY

DATE ISSUED: 13th March 2023

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Fortinet has released a patch for a critical vulnerability in FortiOS and FortiProxy which impacts the Graphical User Interface (GUI) of vulnerable devices. Exploitation can occur without authentication to execute arbitrary code or perform a Denial-of-Service (DoS) attack by crafting malicious request.

BREAKDOWN

The vulnerability is tracked as CVE-2023-25610 and has a CVSS score of 9.3. It is a buffer underflow vulnerability that occurs when the buffer – the temporary holding space during data transfer is fed data at a lower rate than it is being read from. This results in the program or device reading from the buffer to pause leading to risky behaviour or crashes. The bug impacts FortiOS versions 7.2.0 through 7.2.3, 7.0.0 – 7.0.9, 6.4.0 – 6.4.11, 6.2.0 – 6.2.12, and all 6.0 versions. FortiProxy versions 7.2.0 – 7.2.2, 7.0.0 – 7.0.8, 2.0.0 – 2.0.11, all 1.2 versions, and all 1.1 versions are also impacted. This critical-severity vulnerability may provide a method to gain initial access to corporate network which may result in further exploitation and the establishment of persistence or a backdoor, so it is highly recommended to apply the available patch as soon as possible to mitigate this.

REMEDIATION STEPS

- Update and patch the FortiOS and FortiProxy to the latest version.
- If scheduling the update takes an extended time-period, disable the HTTP/HTTPS administrative interface.
- Limit the IP address that can remotely reach the administrative interface of the affected devices.
- Schedule regular malware and vulnerability scans to provides an opportunity to mitigate potential security flaws proactively.
- Network monitoring and analysis should be conducted regularly to detect any anomalous behaviour.

REFERENCES & RESOURCES

Bleeping Computer https://www.bleepingcomputer.com/news/security/fortinet-warns-of-new-critical-unauthenticated-rce-vulnerability/