Cyber Threat Advisory

16 January 2025

TLP:CLEAR

FortiOS & FortiProxy - Authentication bypass in Node.js websocket module vulnerability

This advisory is relevant to Samoan organisations who manage Fortinet Firewalls. This alert is intended to be understood by technical users. Relevant organisations are strongly advised to upgrade to the latest version of FortiOS and FortiProxy and apply the mitigations, as detailed in the Fortinet notification.

What's Happened?

Fortinet has identified a critical vulnerability in FortiOS and FortiProxy and has observed active exploitation of this vulnerability. The vulnerability may allow an unauthenticated remote attacker to gain "super-admin" privileges to the firewall device. This is typically used as an initial access vector for threat actors to gain access to target environments. Devices running FortiOS 7.0.0 through 7.0.16 and FortiProxy version 7.0.0 through 7.0.19 and 7.2.0 through 7.2.12 may be affected. More information on the vulnerability can be found in the National Vulnerability Database. The Fortinet vulnerability notification published by the vendor describes possible Indicators of Compromise (IOCs) and IPs associated the threat actor, which may assist in identifying suspicious activity on potentially affected Fortinet devices.

How do I stay secure?

SamCERT advises that organisations and government departments implement the following controls to determine if you are affected, and to **detect** for instances of exploitation of FortiOS and FortiProxy devices and to **limit its effectiveness**:

Determine Potential Impact:

1. Where you are using Fortinet Firewall devices, login to the device and review the firmware version to determine if the device is susceptible to the exploit.
2. Determine the risk factors associated with upgrading the device.

Enhancing Detection:

1. Where you manage a potentially affected Fortinet device, Investigate for potential compromise by reviewing the Fortinet published IOCs.
2. Monitor and investigate for suspicious activity in connected environments.

Mitigating Controls:

1. Follow Fortinet's published advice for affected versions.
2. Upgrade to the latest FortiOS and FortiProxy versions using the recommended upgrade tool.
3. Where updates are not possible, follow Fortinet's recommended workarounds.
4. Follow the Fortinet Hardening Guidelines located in the Fortinet Document Library.

Further information and details can be found in Fortinet's vulnerability notification.

Where can I go for help?

If you have been impacted by the FortiOS and FortiProxy vulnerability we encourage you to submit a report at:

www.samcert.gov.ws/report-incident

If you require more information, please contact SamCERT on:

samcert@mcit.gov.ws

+685 26 117

TLP:CLEAR