CVE-2024-40591

Escalation Of Privilege (FortiOS)

Vairav Advisory Report

Date: February 14, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

A high-severity privilege escalation vulnerability (CVE-2024-40591) has been identified in FortiOS security fabric. The flaw allows an authenticated administrator with Security Fabric permissions to escalate their privileges to super-admin by connecting the targeted FortiGate to a malicious upstream FortiGate under their control. Organizations using affected versions are strongly advised to apply the recommended updates immediately.

VULNERABILITY DETAILS

CVE-2024-40591

Description: An incorrect privilege assignment vulnerability in the FortiOS security fabric allows an authenticated administrator with Security Fabric permissions to escalate their privileges to super-admin by linking the targeted FortiGate to a malicious upstream FortiGate.

Impact: Privilege escalation, unauthorized administrative access.

CVSS Score: 8.0 (High)

AFFECTED VERSIONS

FortiOS:

- 7.6.0 (Fixed in 7.6.1)
- 7.4.0 through 7.4.4 (Fixed in 7.4.5)
- 7.2.0 through 7.2.9 (Fixed in 7.2.10)
- 7.0.0 through 7.0.15 (Fixed in 7.0.16)
- 6.4 (All versions - Migrate to a fixed release)

EXPLOIT DETAILS

An authenticated administrator with Security Fabric permissions can exploit this vulnerability by linking a targeted FortiGate to a malicious upstream FortiGate, thereby escalating privileges to super-admin. This could lead to full administrative control over the affected system.

RECOMMENDED ACTIONS

Patch & Upgrade:

- Fortinet has released patches to mitigate this vulnerability. Users should upgrade to the latest fixed versions.

ADDITIONAL SECURITY MEASURES

- Restrict administrative access to trusted users and networks.
- Implement role-based access control (RBAC) to limit Security Fabric permissions.
- Enable security logs to detect unauthorized configuration changes.

REFERENCES

https://hackread.com/fortios-vulnerability-super-admin-privilege-escalation/

https://nvd.nist.gov/vuln/detail/cve-2024-40591

https://fortiguard.fortinet.com/psirt/FG-IR-24-302

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com