CVE-2025-24472:

AUTHENTICATION BYPASS IN FORTIOS AND FORTIPROXY

Vairav Advisory Report

Date: 2025-02-12

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148
Baluwatar, Kathmandu

Phone: +977 4541540
Mobile: +977-9820105900
Email: mail@vairavtech.com

EXECUTIVE SUMMARY

A critical vulnerability, identified as CVE-2025-24472, has been discovered in Fortinet's FortiOS and FortiProxy products. This authentication bypass vulnerability allows remote attackers to gain super-admin privileges via crafted CSF proxy requests. The vulnerability has a CVSS score of 8.1 (Critical). Exploitation of this flaw could lead to complete system compromise, unauthorized configuration changes, and unauthorized access to sensitive data.

VULNERABILITY DETAILS

CVE-2025-24472

- **Description:** An Authentication Bypass Using an Alternate Path or Channel vulnerability (CWE-288) exists in some versions of FortiOS and FortiProxy. A remote attacker can exploit this vulnerability by sending specially crafted CSF proxy requests, allowing them to gain super-admin privileges without proper authentication.
- **Impact:** Successful exploitation enables attackers to create unauthorized administrative accounts, modify firewall policies and configurations and access SSL VPN instances using rogue accounts, potentially leading to further network infiltration.
- **CVSS Score:** 8.1 (Critical)

AFFECTED VERSIONS

The following versions are affected by CVE-2025-24472:

- **FortiOS:** 7.0.0 through 7.0.16
- **FortiProxy:** 7.2.0 through 7.2.12 and 7.0.0 through 7.0.19

EXPLOIT DETAILS

Attackers can use this vulnerability alongside CVE-2024-55591 to generate random admin or local users on affected devices, adding them to new and existing SSL VPN user groups. They have also been seen modifying firewall policies and other configurations and accessing SSLVPN instances with previously established rogue accounts "to gain a tunnel to the internal network."

RECOMMENDED ACTIONS

Patch & Upgrade:

Fortinet has released patches to address this vulnerability. Users are strongly advised to upgrade to the latest versions:

- **FortiOS:** Upgrade to version 7.0.17 or later.
- **FortiProxy:** Upgrade to version 7.2.13 or later for the 7.2.x branch, and to version 7.0.20 or later for the 7.0.x branch.

ADDITIONAL SECURITY MEASURES

- **Restrict Administrative Access:** Disable HTTP/HTTPS administrative interfaces or limit access to trusted IP addresses using local-in policies.
- **Monitor for Indicators of Compromise (IoCs):** Review logs for unusual administrative activities.
- **Implement Strong Administrative Practices:** Use non-standard, complex usernames and enforce strong, unique passwords for all administrative accounts.

REFERENCES

- https://app.opencve.io/cve/CVE-2025-24472
- https://www.fortiguard.com/psirt/FG-IR-24-535
- https://nvd.nist.gov/vuln/detail/CVE-2025-24472
- https://www.bleepingcomputer.com/news/security/fortinet-warns-of-new-zero-day-exploited-to-hijack-firewalls/

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: mail@vairavtech.com

Website: https://vairavtech.com