CVE-2024-46662: Escalation Of Privilege In FortiManager

Vairav CVE Report

Date: March 17th, 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 critical vulnerability, **CVE-2024-46662**, has been identified in Fortinet's FortiManager and FortiManager Cloud products. This command injection vulnerability allows authenticated attackers to escalate privileges by sending specifically crafted packets. The vulnerability has been assigned a **CVSS base score of 8.8**, categorized as High severity. Exploitation of this vulnerability could lead to unauthorized command execution, potentially compromising the affected system's integrity and availability.

VULNERABILITY DETAILS

CVE-2024-46662

- **Description:** This vulnerability arises from improper neutralization of special elements used in a command ('command injection') within FortiManager's csfd daemon. An authenticated attacker can exploit this flaw by sending specifically crafted packets, leading to unauthorized command execution on the system.
- **Impact:** Successful exploitation allows attackers to execute arbitrary commands with elevated privileges, potentially leading to full system compromise, unauthorized access to sensitive data, and disruption of services.
- **CVSS Score:** 8.8 (High)

AFFECTED VERSIONS

The following versions of FortiManager and FortiManager Cloud are affected:

- **FortiManager** versions 7.4.1 through 7.4.3
- **FortiManager Cloud** versions 7.4.1 through 7.4.3

EXPLOIT DETAILS

In environments where FortiManager is deployed for centralized management of Fortinet devices, an authenticated attacker with network access can exploit this vulnerability by sending specially crafted packets to the csfd daemon. This could result in unauthorized command execution, leading to privilege escalation and potential full system compromise. The attack complexity is low, and no user interaction is required, making exploitation more feasible.

RECOMMENDED ACTIONS

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

- **FortiManager** version 7.4.4 or later
- **FortiManager Cloud** version 7.4.4 or later

ADDITIONAL SECURITY MEASURES

- **Network Segmentation:** Implement network segmentation to limit access to FortiManager systems, ensuring only authorized personnel can communicate with these management interfaces.
- **Access Controls:** Enforce strict access controls and authentication mechanisms to minimize the risk of unauthorized access.
- **Monitoring and Logging:** Enable comprehensive logging and monitor logs for suspicious activities related to FortiManager systems.

REFERENCES

- https://app.opencve.io/cve/CVE-2024-46662
- https://fortiguard.fortinet.com/psirt/FG-IR-24-222
- https://www.tenable.com/cve/CVE-2024-46662

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