Critical Vulnerabilities In Fortinet Products

Vairav Advisory Report

Date: February 04, 2025

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

CVE-2024-48884, CVE-2024-48885, CVE-2024-48886, and CVE-2024-50563 are critical vulnerabilities affecting multiple Fortinet products, including FortiManager, FortiOS, FortiProxy, FortiManager Cloud, FortiAnalyzer, FortiRecorder, FortiWeb, and FortiVoice. CVE-2024-48884 and CVE-2024-48885 are path traversal vulnerabilities in the csfd daemon, which allow remote authenticated attackers with access to the security fabric interface and port to write arbitrary files. Additionally, remote unauthenticated attackers with the same network access may delete arbitrary folders or escalate privileges via specially crafted packets. CVE-2024-48886 and CVE-2024-50563 are weak authentication vulnerabilities in the csfd daemon, which could allow an unauthenticated attacker to brute-force the authentication process in the Security Fabric protocol, potentially taking control of connected devices. Fortinet has released patches to address these issues, and users are strongly advised to update their systems immediately.

VULNERABILITY DETAILS

CVE-2024-48884

Description: A path traversal vulnerability due to improper pathname restriction allows attackers to escalate privileges via specially crafted packets.

Impact: Escalation of privilege

CVSS Score (NVD): 9.1 (Critical)

CVE-2024-48885

Description: A path traversal vulnerability in FortiRecorder, FortiWeb, and FortiVoice, which allows an attacker to escalate privileges via specially crafted packets.

Impact: Escalation of privilege

CVSS Score (NVD): 9.1 (Critical)

CVE-2024-48886

Description: A weak authentication vulnerability in Fortinet products, may allow an attacker to execute unauthorized code or commands via a brute-force attack.

Impact: Execute unauthorized code or commands

CVSS Score (NVD): 9.8 (Critical)

CVE-2024-50563

Description: A weak authentication vulnerability in FortiManager Cloud, FortiAnalyzer, and FortiManager that allows an attacker to execute unauthorized code or commands via a brute-force attack.

Impact: Execute unauthorized code or commands

CVSS Score (NVD): 9.8 (Critical)

AFFECTED VERSIONS

For CVE-2024-48884 and CVE-2024-48885

- **FortiManager**: 7.6.0 - 7.6.1, 7.4.1 - 7.4.3
- **FortiManager Cloud**: 7.4.1 - 7.4.3
- **FortiOS**: 7.6.0, 7.4.0 - 7.4.4, 7.2.0 - 7.2.9, 7.0.0 - 7.0.15
- **FortiProxy:** 7.4.0 - 7.4.5, 7.2.0 - 7.2.11, 7.0.0 - 7.0.18
- **FortiRecorder**: 7.2.0 - 7.2.1, 7.0.0 - 7.0.4
- **FortiVoice**: 7.0.0 - 7.0.4, 6.4.0 - 6.4.9
- **FortiWeb**: 7.6.0, 7.4.0 - 7.4.4

For CVE-2024-48886 and CVE-2024-50563

- **FortiManager:** 7.6.0 - 7.6.1, 7.4.1 - 7.4.3
- **FortiManager Cloud:** 7.4.1 - 7.4.3
- **FortiOS:** 7.6.0, 7.4.0 - 7.4.4, 7.2.5 - 7.2.9, 7.0.0 - 7.0.15, 6.4.0 - 6.4.15
- **FortiProxy:** 7.4.0 - 7.4.5, 7.2.0 - 7.2.11, 7.0.0 - 7.0.18, 2.0.0 - 2.0.14, 1.2.0 - 1.2.13, 1.1.0 - 1.1.6, 1.0.0 - 1.0.7
- **FortiAnalyzer Cloud:** 7.4.1 - 7.4.3
- **FortiAnalyzer:** 7.6.0 - 7.6.1, 7.4.1 - 7.4.3
- **FortiRecorder:** 7.2.0 - 7.2.1, 7.0.0 - 7.0.4
- **FortiWeb:** 7.6.0, 7.4.0 - 7.4.4, 7.2.0 - 7.2.10, 7.0.0 - 7.0.10, 6.4.0 - 6.4.3
- **FortiVoice:** 7.0.0 - 7.0.4, 6.4.0 - 6.4.9, 6.0.0 - 6.0.12

EXPLOIT DETAILS

Attackers can exploit these vulnerabilities by sending specially crafted network packets to vulnerable devices. These flaws may lead to unauthorized access, modification of system files, privilege escalation, or brute-force authentication bypass and execution of unauthorized commands.

RECOMMENDED ACTIONS

- Fortinet has released patches to mitigate these vulnerabilities. Users should upgrade to the latest available versions of their affected products.

ADDITIONAL SECURITY MEASURES

- Enforce strong authentication methods, including multi-factor authentication (MFA).
- Disable the security fabric using the following commands:

```
config system csf
set status disable
end
```

- Remove the fabric from the config system interface using the following commands:

```
config system interface
edit “portX”
set allow-access ssh https
next
end
```

REFERENCES

https://app.opencve.io/cve/CVE-2024-48884

https://app.opencve.io/cve/CVE-2024-48886

https://nvd.nist.gov/vuln/detail/CVE-2024-48884

https://nvd.nist.gov/vuln/detail/CVE-2024-48886

https://nvd.nist.gov/vuln/detail/CVE-2024-48885

https://nvd.nist.gov/vuln/detail/CVE-2024-50563

https://fortiguard.fortinet.com/psirt/FG-IR-24-259

https://fortiguard.fortinet.com/psirt/FG-IR-24-221

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