# THREAT BULLETINS

## Critical Fortinet Vulnerability (CVE-2024-23113) Under Active Exploitation

TLP:WHITE

Oct 10, 2024

On October 9, 2024, the Cybersecurity and Infrastructure Security Agency (CISA) added CVE-2024-23113 to its known exploited vulnerabilities catalog. The security flaw affects multiple Fortinet products, including FortiOS, FortiPAM, FortiProxy, and FortiWeb.

Despite Fortinet's disclosure and release of patches for the vulnerability back in February, CISA has added it to the catalog because it has evidence that it is being actively exploited in the wild.

The vulnerability is a remote code execution (RCE) security flaw that allows threat actors to execute arbitrary code on unpatched devices, potentially leading to complete system compromise.

Health-ISAC provides this information for situational awareness and encourages users to upgrade affected Fortinet products.

A critical vulnerability affecting multiple Fortinet products was recently added to CISA's known exploited vulnerabilities catalog citing evidence of active exploitation by threat actors.

The vulnerability is caused by the fgfmd daemon accepting an externally controlled format string as an argument. Successful

exploitation allows an unauthenticated threat actor to execute commands or arbitrary code on affected devices in low-complexity attacks without requiring user interaction.

The following products and associated versions are affected:

- FortiOS 7.0 and later
- FortiPAM 1.0 and higher
- FortiProxy 7.0 and above
- FortiWeb 7.4

The vulnerable fgfmd daemon operates on FortiGate and FortiManager devices. It is responsible for handling all authentication requests and managing communication between these devices for tasks such as instructing other processes to update files or databases.

**Recommendations:**

Health-ISAC recommends organizations review and assess their level of risk to this vulnerability and take the necessary actions to ensure appropriate security measures are implemented, including:

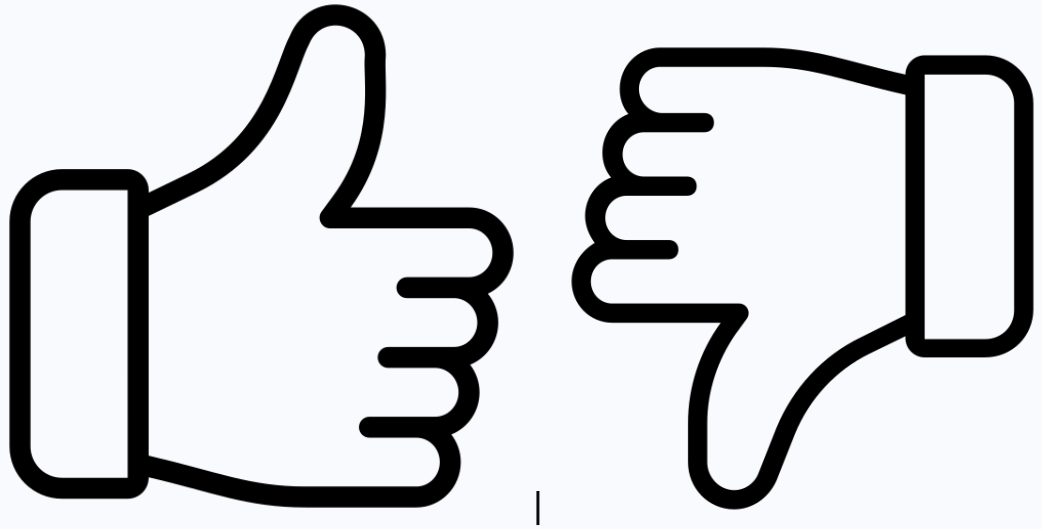
- Immediately apply available patches for affected versions.
    - If patching is not feasible, admins can apply the following workaround:
- Remove fgfm access for each interface.
- Apply the principle of least privilege to minimize the potential impact if exploitation occurs.
- Review the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Resources.

| | |
|---|---|
| **Reference(s)** | Bleeping Computer, Security Week, Fortiguard, cybersecuritynews, CISA, CISA, HHS |

**Alert ID** 824d7fad

## View Alert

Share Feedback
was this helpful?



**Tags** CVE-2024-23113, Fortinet

**TLP:WHITE** Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

**Access the Health-ISAC Threat Intelligence Portal**
Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

**For Questions or Comments**
Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**