THREAT BULLETINS

Update: Fortinet Notifies Customers about an Exploited 0-Day Flaw in FortiManager

TLP:WHITE

Oct 24, 2024

Update:

On October 23, Fortinet published an advisory for the critical vulnerability in the FortiManager fgfmd daemon. The flaw, tracked as CVE-2024-47575, is being actively exploited. Its CVSS score of 9.8 highlights its criticality.

The vulnerability is related to the FortiGate to FortiManager (FGFM) protocol, allowing remote unauthenticated attackers to execute arbitrary code or commands. According to the advisory, identified attacks in the wild used scripts to automate the exfiltration of sensitive data, such as files located on FortiManager, which included IPs, credentials, and configurations of the managed devices. Currently, no evidence suggests the flaw has been used to deploy malware or backdoors.
Furthermore, Fortinet warns that restoring a backup from a compromised system may reintroduce tampered data. The FortiGate's activity log should be verified to check for unauthorized access since data may have been exfiltrated. Passwords and sensitive data of managed devices should be changed urgently. To recover from a compromised FortiManager instance, keep a copy in an isolated network and compare it with the new setup. It is recommended to use offline and closed-network modes for operation.

Recommendations:

- *Apply available patches issued by Fortinet.*
- *Check your system for IoCs from the advisory and verify the activity log to ensure no compromise has happened.*
- *Change all passwords on the affected devices.*
- *Segment your networks to minimize the risk of lateral movement.*
- *Enforce network segmentation and strict network access control policies.*
- *Implement MFA and limit account privileges.*
- *Continuously monitor for suspicious activities.*
- *Have an incident response plan ready to limit operational disruptions in the event of a successful attack.*
- *Review the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients resources.*

Original alert:

On October 22, 2024, ArsTechnica shared an article titled FortiGate admins report active exploitation 0-day. Vendor isn't talking. The article details a recent discovery impacting Fortinet FortiManager.

Fortinet has privately notified its customers about a significant vulnerability threat that actors exploited to run malicious code on servers used by sensitive customer organizations. This was discovered via one of the customer's Reddit posts.

The initial disclosure to the customers was reported on October 15, while the company has not yet made any public announcements about the CVE or the exploitation.

Health-ISAC is sharing this bulletin to ensure teams are tracking the developing threat.

According to the aforementioned Reddit post, the vulnerability allegedly affects FortiManager, a software tool for managing all traffic and devices on an organization's network.

The affected products are:

- FortiManager versions 7.6.0 and below
- FortiManager versions 7.4.5 and below
- FortiManager versions 7.2.7 and below
- FortiManager versions 7.0.12 and below
- FortiManager versions 6.4.14 and below

As of this writing, 3 of the impacted versions don't yet have patches available. Patches for 7.4.5 and 7.2.7 are available. To mitigate the flaw in versions that have patches, users are advised to install versions 7. 6. 1 or higher to protect themselves.

Independent researcher Kevin Beaumont shared on Mastodon that FortiManager is vulnerable due to a default setting that permits devices with unrecognized serial numbers to register themselves on an organization's dashboard. The vulnerability is connected to FortiGate to FortiManager Protocol (FGFM). The FortiManager unit's Device Manager uses FGFM to help configure the device. This protocol operates on port 541. Beaumont further indicates in his Medium blog post that according to Shodan, there are 60,000 FGFM instances exposed to the internet and hence vulnerable to attacks.

Other security researchers have suggested that incidents involving the flaw may involve certificate theft. However, none of this information has been confirmed, and there is currently no official information detailing the nature of these attacks.
Health-ISAC recommends applying available patches and possibly shutting off affected FortiManager devices from the public internet until more details are publicly available.

There is currently no information from Fortinet and the Fortinet PSIRT webpage is currently offline.

Recommendations:

- Apply available patches for vulnerable FortiManager devices.
- Switch off vulnerable devices that do not have available patches from the internet.
- Stay vigilant for any email communication from Fortinet regarding the flaw.
- Segment your networks to minimize the risk of lateral movement.

- Enforce network segmentation and strict network access control policies.
- Implement MFA and limit account privileges.
- Continuously monitor for suspicious activities.
- Have an incident response plan ready to limit operational disruptions in the event of a successful attack.
- Review the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients resources.

Reference(s)	Fortiguard, cyberplace, infosec, Double Pulsar, Ars Technica

Sources

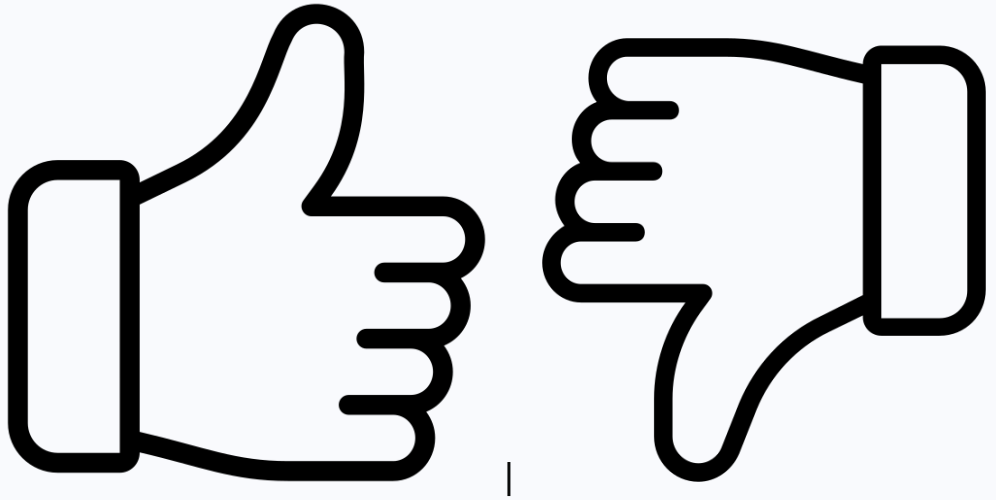
CISA Adds One Known Exploited Vulnerability to Catalog
Fortinet's Advisory
Fortinet Warns of Critical Vulnerability in FortiManager Under Active Exploitation

Incident Date
Oct 24, 2024 (UTC)

Alert ID 2aecf308

View Alert

Share Feedback
was this helpful?



Tags FortiManager, Fortinet

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

Share Threat Intel
For guidance on sharing indicators with Health-ISAC via HTIP, please visit the Knowledge Base article "HTIP - Share Threat Intel" here.

The "Share Threat Intel" feature allows for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

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/**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.