Critical Vulnerabilities in Fortinet's FortiMonitorOnSight and Privileged Access Agent Chrome Extension (CVE-2026-84390 & CVE-2026-84388)

Sep 10, 2026

View Alert

WHITE

Fortinet has issued security updates addressing 10 vulnerabilities across various products. Key flaws include an **authentication bypass flaw** in the **FortiMonitorOnSight** web portal that uses forged JSON Web Tokens **(CVE-2026-84390)** and a proxy flaw in the **Fortinet Privileged Access Agent Chrome extension (CVE-2026-84388)** that can divert browser traffic to malicious websites. **A complete resolution of the extension issue requires updating both FortiPAM and the Chrome plugin.**

Additional updates resolve medium to high-risk flaws in **FortiSandbox**, **FortiOS**, **FortiManager**, and other products, preventing potential unauthorized code execution, traffic interception, or service disruptions. Fortinet has reported no active exploitation.

Additional Info

Analysis:

Fortinet recently issued security updates addressing ten (10) software flaws across its product portfolio. The updates address notable vulnerabilities, including an **authentication bypass** issue in the **FortiMonitorOnSight** web portal, tracked as **CVE-2026-84390**, and an **improper authentication bug** in the **Fortinet Privileged Access Agent Chrome extension**, tracked as **CVE-2026-84388**.

Additional updates target information exposure in FortiSandbox and man-in-the-middle risks in the FortiOS and FortiProxy Agentless ZTNA portals. Other fixed issues involve low-to-medium risk conditions across central management, SIEM, and analytics platforms, with no active exploitation reported in the wild.

For health sector organizations, these updates carry operational significance given the industry's reliance on continuous network availability and the protection of sensitive data. Vulnerabilities that enable authentication bypass or traffic proxying could expose patients' electronic health records (EHRs) and administrative systems to unauthorized access. Furthermore, potential denial-of-service conditions or system instability could disrupt clinical workflows and real-time monitoring tools. Because healthcare IT environments often blend cloud services, remote clinical access, and physical medical devices, security weaknesses in identity verification, proxy routing, or remote access agents expand the potential attack surface across clinical networks.

Recommendations and Mitigations:

Health-ISAC recommends organizations review and assess their risk exposure to these vulnerabilities and implement the following:

- **Upgrade FortiPAM and Chrome Extension:** Update FortiPAM to version 1.9.1 or 1.8.4, and ensure the Fortinet Privileged Access Agent extension is at version 8.0.1.123 or higher.
- **Patch ZTNA and FortiSandbox Portals:** Apply the latest security updates to FortiSandbox, FortiOS, and FortiProxy Agentless ZTNA portals to protect against potential traffic interception and information exposure.
- **Patch Central Management Systems:** Update remaining affected software, including FortiManager, FortiAnalyzer, FortiSIEM, and FortiSOAR, during upcoming maintenance windows.

- **Validate Access and Token Policies:** Review authentication configurations and JSON Web Token (JWT) handling to prevent unauthorized access bypasses.
- **Monitor Administrative Logs:** Audit network logs and SIEM consoles for unusual proxy requests, unexpected session activity, or unverified logins across critical health infrastructure.
- **Review the Health Industry Cybersecurity Practices (HICP):** Managing Threats and Protecting Patients Resources.

<hr size=1 width="100%" align=center>

Alert Id	d48e3b91
Category	Vulnerability Bulletins
References	hhs securityweek fortiguard fortiguard 1
Tags	Privileged Access Agent Chrome Extension, FortiMonitorOnSight, CVE-2026-84390, CVE-2026-84388, Fortinet

---

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

Please provide your feedback

Like Dislike

Download the App

Available on iOS, Android and Web

Download on the App Store Get it on Google Play

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

Health-ISAC is an invite only platform. Please DO NOT forward this email to anyone. If you are not supposed to receive this email, please report to **toc@h-isac.org**

--

partners/010001a089a0d4fe-fa5ca079-2ec0-41d1-a901-466fede970f4-000000%40email.amazonses.com.