Critical and High Severity Vulnerabilities in Several Ivanti's Enterprise Security Products (CVE-2026-12744, CVE-2026-12645, CVE-2026-12646, and more)

Sep 10, 2026

WHITE

View Alert

Ivanti released security updates for **Neurons for ITSM**, **Sentry**, and **Endpoint Manager Mobile (EPMM)** to patch several code-execution and authentication-bypass flaws. Neurons for ITSM addressed eight issues, including unauthenticated and authenticated data deserialization, as well as missing authorization flaws. Sentry and EPMM received patches for high-severity authentication bypasses.

On-premises customers are advised to update to the resolved versions, while cloud environments were patched automatically. Ivanti reports no active exploitation of these issues.

Additional Info

Analysis:

Ivanti has issued security patches addressing multiple software vulnerabilities across its enterprise service management and endpoint mobile management products.

Affected Platforms:

- Neurons for ITSM (Cloud & On-prem)
- Sentry
- Endpoint Manager Mobile (EPMM)

Below is the list of vulnerabilities identified by Ivanti on their Enterprise Security Products:

- **CVE-2026-12650 (CVSS 9.9 - Critical):** A deserialization flaw in Ivanti Neurons for ITSM allows a remote authenticated attacker to execute arbitrary code.
- **CVE-2026-12645 (CVSS 9.9 - Critical):** A missing authorization weakness in Ivanti Neurons for ITSM, allowing a remote authenticated attacker to execute arbitrary code.
- **CVE-2026-12646 (CVSS 9.9 - Critical):** A missing authorization vulnerability in Ivanti Neurons for ITSM permits remote code execution by authenticated users.
- **CVE-2026-12647 (CVSS 9.9 - Critical):** A missing authorization security issue in Ivanti Neurons for ITSM allows authenticated remote code execution.
- **CVE-2026-12744 (CVSS 9.8 - Critical):** A untrusted data deserialization flaw in Ivanti Neurons for ITSM, enabling unauthenticated remote code execution.
- **CVE-2026-12745 (CVSS 9.8 - Critical):** A deserialization flaw in Ivanti Neurons for ITSM allows an unauthenticated remote attacker to execute arbitrary code.
- **CVE-2026-12651 (CVSS 8.8 - High):** A deserialization defect in Ivanti Neurons for ITSM allows authenticated remote code execution.
- **CVE-2026-12648 (CVSS 8.8 - High):** A deserialization vulnerability in Ivanti Neurons for ITSM, allowing authenticated remote code execution.

Most identified security flaws affect on-premises **Neurons for ITSM** instances, enabling remote code execution through improper authorization or the handling of untrusted data. SaaS environments were remediated directly by the vendor in August 2026. Currently, there is no evidence of active exploitation in production environments.

In healthcare environments, ITSM and mobile management software govern operational workflows, incident routing, and device policies associated with clinical systems. System flaws that permit unauthorized code execution create operational risk if public-facing service management consoles are left unsegmented. Unauthenticated entry points allow unauthorized network access, while authenticated flaws increase exposure to the compromise of user credentials. Maintaining strict perimeter controls around enterprise management servers remains a critical line of defense against network intrusion.

Recommendations and Mitigations:

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

- **Apply Security Patches:** Update on-premises instances of Ivanti Neurons for ITSM, Sentry, and Endpoint Manager Mobile (EPMM) to the latest resolved software releases immediately.
- **Restrict Internet Exposure:** Ensure on-premises ITSM portals and administrative consoles are not directly accessible from the public internet. Secure them behind firewalls, internal networks, or secure VPN gateways.
- **Monitor Authentication and Access Logs:** Review system and authentication logs across Sentry and EPMM platforms for unexpected administrative access or credential misuse.
- **Enforce Least Privilege and MFA:** Enforce strict access control policies and multi-factor authentication for service management and device management tools to limit exposure to authenticated code execution flaws.
- **Review the Health Industry Cybersecurity Practices (HICP):** Managing Threats and Protecting Patients Resources.

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

Alert Id	3930b88a
Category	Vulnerability Bulletins
References	ivanti hhs securityweek
Tags	Ivanti Sentry, CVE-2026-12744, CVE-2026-12645, CVE-2026-12646, Neurons for ITSM, Ivanti Endpoint Manager Mobile (EPMM), Ivanti Endpoint Manager Mobile, Ivanti

---

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**

--