Cisco Patches 9 High/Maximum Severity Crosswork and Secure Workload Flaws (CVE-2026-20030, CVE-2026-20357, CVE-2026-20358, CVE-2026-20359, and more)

Aug 24, 2026

WHITE

View Alert

Cisco has released security updates addressing several high-severity vulnerabilities discovered during internal testing across its Crosswork and Secure Workload platforms. The flaws involve SQL injection, access control issues, input validation errors, and missing authentication.

Affected products include Crosswork platforms (versions 7.2.1 and earlier, patched in 7.2.1-SP) and Secure Workload releases (patched in 3.10.9.1 and 4.0.4.16). While Cisco reports no known active exploitation for these specific Crosswork and Secure Workload vulnerabilities, users are advised to apply the patches to mitigate risks, especially given recent active exploitation of other Cisco security flaws.

Additional Info

Analysis

Cisco disclosed security updates for Crosswork platforms and Secure Workload Software to remediate internal vulnerabilities before they were publicly exploited.

- **CVE-2026-20030 (CVSS 10.0):** SQL injection vulnerability in Crosswork platforms.
- **CVE-2026-20357 (CVSS 10.0):** Missing authentication for a critical function in Crosswork platforms.
- **CVE-2026-20358 (CVSS 10.0):** External control of file system vulnerability in Crosswork platforms.
- **CVE-2026-20359 (CVSS 9.9):** Insufficiently protected credentials in Crosswork platforms.
- **CVE-2026-20231 (CVSS 9.9):** Command, operating system, and argument injection vulnerabilities in Secure Workload.
- **CVE-2026-20315 (CVSS 10.0):** Improper access control vulnerabilities affecting authorization and privileges in Secure Workload.
- **CVE-2026-20317 (CVSS 10.0):** Improper authentication vulnerabilities, including bypasses in Secure Workload.
- **CVE-2026-20318 (CVSS 9.6):** Improper input validation and path traversal flaws in Secure Workload.
- **CVE-2026-20319 (CVSS 7.5):** Buffer overflow and out-of-bounds write memory flaws in Secure Workload.

In health sector environments, network automation and workload protection tools manage connected medical infrastructure, patient data repositories, and administrative networks. Flaws affecting access controls, authentication mechanisms, and command execution on these management platforms create pathways that unauthorized actors could leverage to disrupt healthcare operations or access sensitive patient information. Because medical systems depend heavily on continuous network stability and data privacy, vulnerabilities in infrastructure management software can expose health organizations to operational downtime and regulatory non-compliance if left unaddressed. Proactive mitigation is essential to maintaining the integrity and availability of patient services.

Recommendations

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

- **Update Software Immediately:** Patch Cisco Crosswork platforms to version 7.2.1-SP, and Cisco Secure Workload deployments to version 3.10.9.1 or 4.0.4.16.
- **Enforce Network Segmentation:** Restrict access to network management interfaces and isolate core administrative controllers from general hospital networks.
- **Review System Logs:** Audit authentication logs, file system activity, and API requests on affected systems for unusual behavior or unauthorized access attempts.
- **Coordinate Patch Timelines:** Schedule maintenance windows with clinical leadership to prevent software updates from interrupting patient care or critical medical systems.
- **Restrict Access Credentials:** Apply the principle of least privilege across all network automation and workload management interfaces.
- **Monitor Infrastructure Continuously:** Utilize automated network monitoring tools to detect anomalous traffic patterns and potential lateral movement within health systems.
- **Reviewing the Health Industry Cybersecurity Practices (HICP):** Managing Threats and Protecting Patients Resources.

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

Alert Id	10a50e63
Category	Vulnerability Bulletins
References	cisco cisco 1 hhs bleepingcomputer
Tags	CVE-2026-20319, CVE-2026-20318, CVE-2026-20317, CVE-2026-20315, CVE-2026-20231, CVE-2026-20359, CVE-2026-20358, CVE-2026-20357,

CVE-2026-20030, Cisco Crosswork, Cisco Secure Workload, Cisco

---

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

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**

--