



# VULNERABILITY BULLETINS

## Cisco Addressed Nine Vulnerabilities Affecting Multiple Products



TLP:WHITE

Sep 12, 2024

On September 11, 2024, Cisco issued [advisories](#) disclosing vulnerabilities affecting multiple products, including Cisco IOS XR Software, Crosswork Network Services Orchestrator (NSO), Optical Site Manager, and RV340 Dual WAN Gigabit VPN Routers. The vulnerabilities have CVSS scores ranging from 5 to 8.8. Some flaws allow unauthenticated attackers to launch DoS attacks or execute arbitrary code remotely.

The vulnerabilities are:

- CVE-2024-20304 - Cisco IOS XR Software UDP Packet Memory Exhaustion Vulnerability
- CVE-2024-20381 - Multiple Cisco Products Web-Based Management Interface Privilege Escalation Vulnerability
- CVE-2024-20317 - Cisco IOS XR Software Network Convergence System Denial of Service Vulnerability
- CVE-2024-20406 - Cisco IOS XR Software Segment Routing for Intermediate System-to-Intermediate System Denial of Service Vulnerability
- CVE-2024-20398 - Cisco IOS XR Software CLI Privilege Escalation Vulnerability
- CVE-2024-20483 and CVE-2024-20489 - Cisco Routed Passive Optical Network Controller Vulnerabilities

- CVE-2024-20390 - Cisco IOS XR Software Dedicated XML Agent TCP Denial of Service Vulnerability
- CVE-2024-20343 - Cisco IOS XR Software CLI Arbitrary File Read Vulnerability

There are currently no reports of any of the flaws being exploited. Health-ISAC recommends applying available updates as soon as possible as the most effective prevention from cyberattacks.

### **Recommendations**

Members are additionally advised to review Health Industry Cybersecurity Practices (HICP): [Managing Threats and Protecting Patients Resources](#) for additional guidance on how to keep organizations safe from cyberattacks.

Source:

#### **Reference(s)**

[Security Week](#), [mimecastprotect](#), [Security Online](#), [Cisco](#)

### **Sources**

[Cisco Issues Security Advisories: Critical Vulnerabilities Impact Multiple Products](#)

[Cisco Security Advisories](#)

[Cisco Patches High-Severity Vulnerabilities in Network Operating System](#)

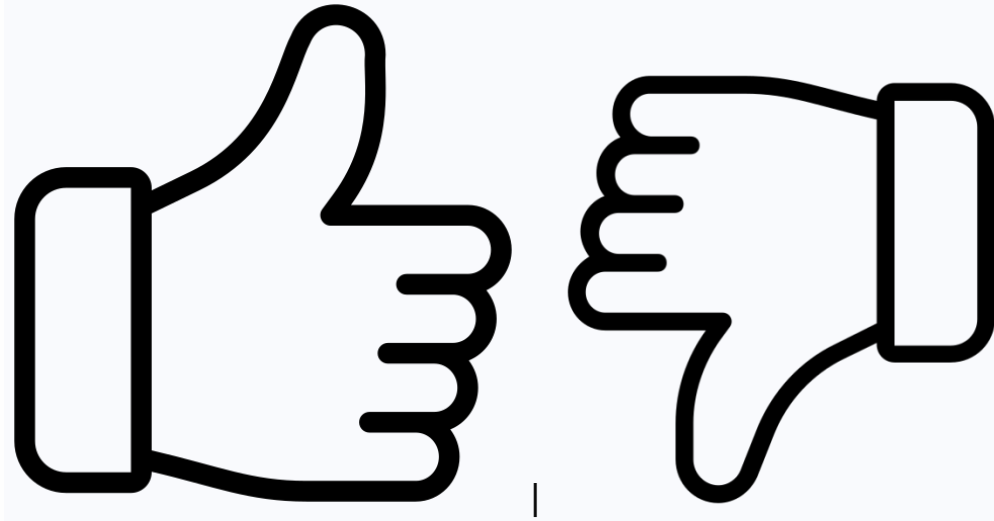
### **Release Date**

Sep 12, 2024 (UTC)

**Alert ID** e01fee24

**[View Alert](#)**

Share Feedback  
was this helpful?



**Tags** RV340 Dual WAN Gigabit VPN Routers, Optical Site Manager, Crosswork Network Services Orchestrator (NSO), IOS XR Software, 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](mailto: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](mailto: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](mailto:toc@h-isac.org).

Powered by [Cyware](#)

