October 16, 2023

Overall rating: Critical

BRITISH COLUMBIA

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware Cisco has published a Security. Bulletin to address vulnerabilities in Cisco Emergency Responder Vulnerabilities.

Technical Details

On October 16, 2023, Cisco published a security advisory to address a vulnerability in the following product:

- Cisco IOS XE – all versions

Cisco is aware of active exploitation of a previously unknown vulnerability in the web UI feature of Cisco IOS XE Software when exposed to the internet or to untrusted networks. This vulnerability allows a remote, unauthenticated attacker to create an account on an affected system with privilege level 15 access. The attacker can then use that account to gain control of the affected system.

For steps to close the attack vector for this vulnerability, see the Recommendations section of this advisory

Cisco will provide updates on the status of this investigation and when a software patch is available.

This vulnerability is rated as a **Critical** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify VRM with any questions or concerns you may have.

References

- CVE-2023-20198
- Cisco Security Advisory - cisco-sa-iosxe-webui-privesc-j22SaA4z
- Cisco Security Advisories

Please note that we will be transitioning to a new site on August 31, 2023, where we will post the vulnerability reports.

You will be able to find all the reports that we have published as well as all future reports here: Cybersecurity Alerts

Peter Kremer