HC3 Sector Alert: Critical Vulnerability in Cisco Emergency Responder

Finished Intelligence Reports	TLP:WHITE	Alert Id: b492f5d5	2023-10-10 13:29:39

On October 06, 2023, the Health Sector Cybersecurity Coordination Center (HC3) released a sector alert regarding Critical Vulnerability in Cisco Emergency Responder.

Cisco recently released an update which fixes a critical vulnerability in their Emergency Responder communications platform, a system that is utilized in the health sector. Exploitation of this vulnerability allows for a cyber-attacker to completely compromise a vulnerable system, and then utilize it for further cyberattacks across an enterprise network. HC3 recommends healthcare organizations identify vulnerable systems in their infrastructure and prioritize the implementation of this update.

For additional details, please see the attached report.

Report Source(s): HC3

Release Date: Oct 11, 2023 (UTC)

Tags: Emergency Responder Platform

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions and/or Comments:

Please email us at contact@h-isac.org

Share Threat Intel:

For guidance on sharing indicators with Health-ISAC via CSAP, please visit the Knowledge Base article CSAP ■Share Threat Intel■ Documentation at the link address provided here: https://health-isac.cyware.com/webapp/user/knowledge-base Additionally, this collaborative medium provides opportunities for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

Knowledge Base:

Check out our Knowledge Base for HITS integration documentation. https://health-isac.cyware.com/webapp/user/knowledge-base/f4b0c136/

Access the Health-ISAC 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 Cyware.