HC3: Sector Alert

October 6, 2023 TLP:CLEAR Report: 202310061700

Critical Vulnerability in Cisco Emergency Responder Platform

Executive Summary

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 cyberattacker 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.

Report

This report summarizes Cisco's Unified Communications platform, Cisco's Emergency Responder platform and a crtitical vulnerability in Emergency Responder, which can allow for full compromise of a victim system. HHS recommends prioritizing the mitigation of this vulnerability (specific instructions below). HHS also recommends the operation and maintenance of an enterprise vulnerability management program for all organizations, whether conducted in-house or outsourced, or an implementation of both for a hybrid approach.

Technology Overview

The vulnerable software in question – Cisco's Emergency Responder (CER) communications platform – runs on top of another Cisco platform, their Unified Communications Manager. Cisco's Unified Communications Manager (also known as Cisco Call Manager) is a communications and collboration platform used across industries, including the health sector. Cisco states that "more than 200,000 customers worldwide have deployed over 85 million Cisco IP phones and tens of millions of soft clients." Cisco's Emergency Responder, which is a component of the Unified Communications Manager platform, includes the following functionality:

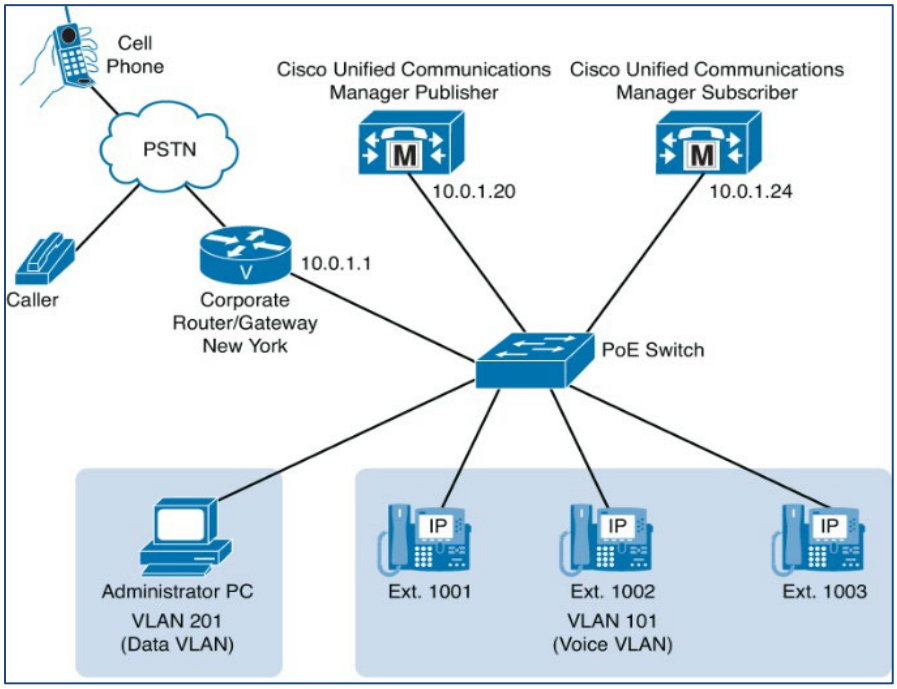

Figure 1: Topology of Cisco Unified Communications Manager. *(Image source: O'Reilly)*

- Emergency Call Routing – This includes calls to public safety personnell as well as other emergency services; these services can be extended to cellular and VOIP phones.
- Database Management – Emergency Responder operates and maintains structured data repositories to support location of phones, call, nature of call, etc.
- Location Tracking – Leveraging database capabilities, Emergency Responder can track locations of stationary (especially VOIP) as well as mobile phones, to facilitate improved response times.

- Alerts/Notifications – Emergency Responder has the ability to relay priority traffic to selected individuals and groups regarding data, such as the location of the caller and the nature of the emergency.

CER is designed to assist organizations in responding promptly and effectively to emergencies by providing accurate location information, and instant and accurate call/communications routing related to the emergencies.

Vulnerability

On October 4, 2023, Cisco released a security advisory regarding a vulnerability in their Emergency Responder platform. Exploitation of this vulnerability can allow an unauthenticated, remote attacker to access the system as root (administrative privileges) and execute arbitrary commands. This vulnerability is tracked as CVE-2023-20101, is rated critical and has a CVSS score of 9.8 out of 10. As the security advisory notes, the root account has default static credentials and cannot be modified or removed. There are no workarounds for this vulnerability. The software must be updated for the vulnerability to be mitigated. This vulnerability is only applicable to Cisco's Emergency Responder Release 12.5(1)SU4.

Patches, Mitigations, and Workarounds

As previously noted, only Cisco's Emergency Responder Release 12.5(1)SU4 is vulnerable. Versions 11.5(1) and earlier, as well as version 12.5(1) and version 14, are not vulnerable. For instructions on updating/patching this vulnerability, the vulnerability alert for CVE-2023-20101 should be consulted.

References

Cisco Emergency Responder Static Credentials Vulnerability
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cer-priv-esc-B9t3hqk9

Cisco Emergency Responder
https://www.cisco.com/c/en/us/products/unified-communications/emergency-responder/index.html

Understand Cisco Emergency Responder (CER)
https://www.cisco.com/c/en/us/support/docs/voice-unified-communications/emergency-responder/116058-cisco-emergency-responder-00.html

Cisco fixes serious flaws in emergency responder and other products
https://www.csoonline.com/article/654740/cisco-fixes-serious-flaws-in-emergency-responder-and-other-products.html

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback