UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0286

CISCO CRITICAL BUGS IN IP PHONES

DATE ISSUED: 6th March 2023

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Cisco released security patch for a critical security vulnerabilty in the web-based management interface of multiple IP phone models. If exploited, this vulnerability could allow an unauthenticated attacker to run Remote Code Execution (RCE) and gain root privilidges on the underlying operating system of an affected device.

BREAKDOWN

An IP Phone system or VoIP phone system functions using Voice over Internet Protocol (VoIP) technology. It allows the user to take incoming calls and make outgoing calls using an internet connection. The first security flaw patched by Cisco is a command injection vulnerability tracked as CVE-2023-20078. This allows an attacker to inject arbitrary commands that are executed with root privilidges which may result in a RCE attack. This vulnerability affects Cisco IP Phone 6800, 7800, and 8800 Series Multiplatform phones. The second vulnerability tracked as CVE-2023-20079 can allow an attacker to cause the affected device to reload, resulting in Denial-of-Service (DoS) attack. It affects Cisco IP Phone 6800, 7800, and 8800 Series Multiplatform Phones, as well as Cisco Unified IP Conference Phone 8831 and Unified IP Phone 7900 Series Phones.

Both vulnerabilities are the result of insufficient validation of user-supplied input and can be exploited using maliciously crafted requests sent to the targeted device's web-based management interface. While Cisco has released security updates to address the CVE-2023-20078 RCE vulnerability, it has stated that it will not release patches to fix the CVE-2023-20079 DoS flaw.

REMEDIATION STEPS

- Disable CDP on affected IP Phone devices supporting Link Layer Discovery Protocol (LLDP) to remove the attack vector.
- Upgrade to the latest version of the software and ensure security patches are supplied.

REFERENCES & RESOURCES

Bleeping Computer	https://www.bleepingcomputer.com/news/security/cisco-patches-critical-web-ui-rce-flaw-in-multiple-ip-phones/