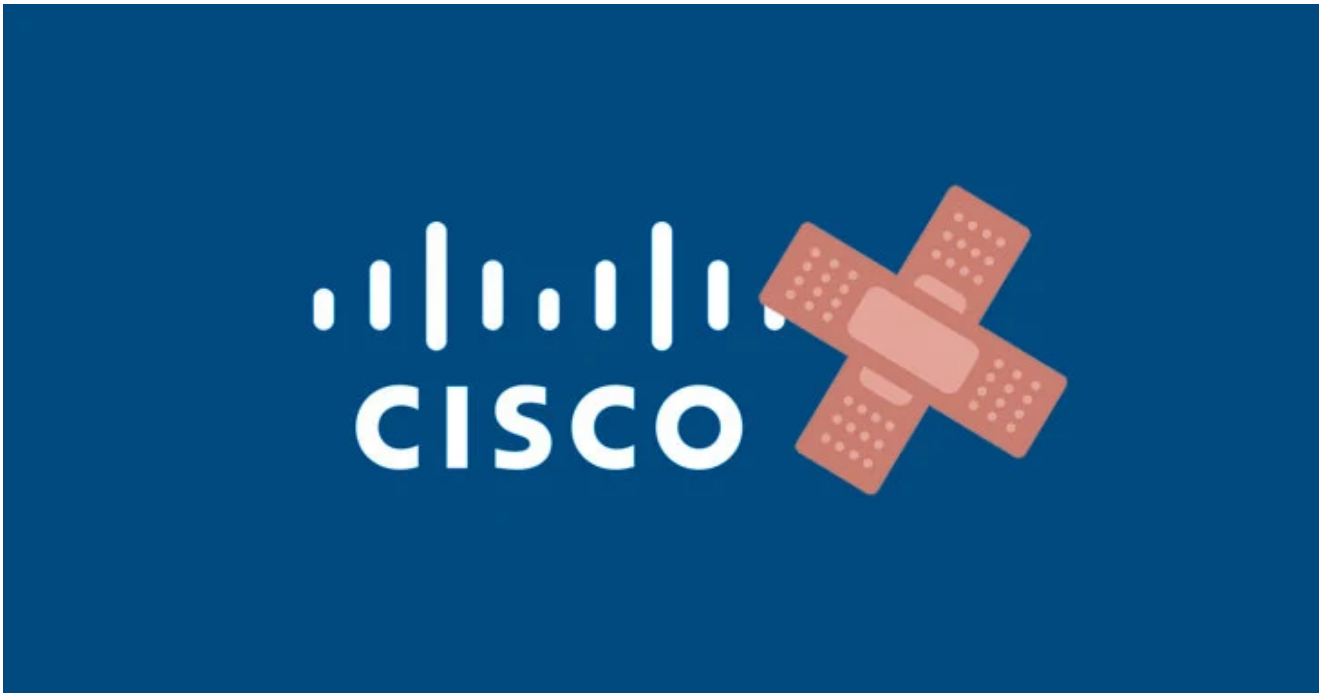
Critical Flaw in Cisco Secure Email and Web Manager Lets Attackers Bypass Authentication

thehackernews.com/2022/06/critical-flaw-in-cisco-secure-email-and.html

June 16, 2022



Cisco on Wednesday rolled out fixes to address a critical security flaw affecting Email Security Appliance (ESA) and Secure Email and Web Manager that could be exploited by an unauthenticated, remote attacker to sidestep authentication.

Assigned the CVE identifier CVE-2022-20798, the bypass vulnerability is rated 9.8 out of a maximum of 10 on the CVSS scoring system and stems from improper authentication checks when an affected device uses Lightweight Directory Access Protocol (LDAP) for external authentication.

"An attacker could exploit this vulnerability by entering a specific input on the login page of the affected device," Cisco noted in an advisory. "A successful exploit could allow the attacker to gain unauthorized access to the web-based management interface of the affected device."

The flaw, which it said was identified during the resolution of a technical assistance center (TAC) case, impacts ESA and Secure Email and Web Manager running vulnerable AsyncOS software versions 11 and earlier, 12, 12.x, 13, 13.x, 14, and 14.x and when the following two conditions are met -

- The devices are configured to use external authentication, and
- The devices use LDAP as authentication protocol

Separately, Cisco also notified customers of another critical flaw affecting its Small Business RV110W, RV130, RV130W, and RV215W routers that could allow an unauthenticated, remote adversary to execute arbitrary code or cause an affected device to restart unexpectedly, resulting in a denial of service (DoS) condition.

The bug, tracked as CVE-2022-20825 (CVSS score: 9.8), relates to a case of insufficient user input validation of incoming HTTP packets. However, Cisco said it neither plans to release software updates nor workarounds to resolve the flaw because the products have reached end-of-life.

Found this article interesting? Follow us on Twitter and LinkedIn to read more exclusive content we post.