Cisco security appliances have critical vulnerabilities

itnews.com.au/news/cisco-security-appliances-have-critical-vulnerabilities-581405

Richard Chirgwin

Cisco has patched its security appliances and told users of some obsolete routers to replace their hardware.

Cisco's Secure Email and Web Manager (formerly known as the Security Management Appliance) and its Email Security Appliance are impacted by CVE-2022-20798, which allows authentication bypass.

If the affected device is using the Lightweight Directory Access Protocol (LDAP) for external authentication, an attacker can enter “a specific input on the login page of the affected device,” Cisco’s advisory states.

“A successful exploit could allow the attacker to gain unauthorised access to the web-based management interface of the affected device.”

If admins can’t patch an affected device immediately, the workaround is to “disable the anonymous binds on the external authentication server”, Cisco said.

The appliances are also subject to CVE-2022-20664, an information disclosure bug that could expose user credentials.

The bug allows “an authenticated, remote attacker to retrieve sensitive information from a LDAP external authentication server connected to an affected device.”

Patches have been released for affected and supported AsyncOS versions.

Owners of the company’s RV110W, RV130, RV130W, and RV215W small business routers will need to replace their hardware, because the other critical vulnerability, CVE-2022-20825, won’t be fixed.

Puzhuo Liu from of the Chinese Academy of Sciences discovered an unauthenticated remote attacker can execute arbitrary code on a victim, or restart the unit causing a denial-of-service.

Because these products have “entered the end-of-life process”, they won’t be patched.