Issued 10/24/17

No Patches for Vulnerabilities in Linksys Wireless Routers

The flaws were reported to Linksys in July and while the vendor was initially responsive, it stopped answering SEC Consult's emails in early September, when it said that patches for some of the vulnerable devices had been on their way to QA.

According to an advisory published by SEC Consult, Linksys E900, E1200 and E8400 AC2400 routers have been confirmed to be vulnerable by the vendor. The security firm conducted its tests on an E2500 device, but it believes E900-ME, E1500, E3200, E4300 and WRT54G2 routers are affected as well. Researchers have discovered a total of five types of vulnerabilities and proof-of-concept (PoC) examples have been made available for each of them. The flaws include denial-of-service (DoS), HTTP header injection, improper session protection, cross-site request forgery (CSRF), and cross-site scripting (XSS) issues.

The security firm has advised users to keep an eye out for the patches from Linksys and apply them as soon as they become available. In the meantime, users can prevent potential attacks by restricting network access to the device.