Three critical holes in Linksys routers, hackers can take advantage of hijacking

Linksys E series routers can get three vulnerabilities that help hackers gain control.

Linksys E series routers can get three vulnerabilities that help hackers gain control. This is security researcher Jared Rittle's discovery by the Cisco Tales Intelligence Group.

Taking advantage of these vulnerabilities, hackers can send an authenticated HTTP request to the network configuration, then he can execute arbitrary system commands on the device.

Incorrect filtering of data and entering NVRAM causes arbitrary system commands to cause these vulnerabilities. Bad guys can send system commands to NVRAM using the data entered into the Domain Name field via the control interface on the web of apply.cgi or Router Name field through the router's web interface.

ilustrační foto

To exploit these vulnerabilities, bad guys must have a password to access the router's console. Currently, many users when buying a router still keep the same account and default password of the manufacturer.

Jared Rittle said Linksys routers are vulnerable to the E series. He performed a successful test on E1200, E2500.

These three errors were reported to Linksys by Cisco Talos on July 9. And Linksys patched the E1200 and E2500 routers on August 14 and October 4 respectively.

According to experts, users who are using Linksys routers with three vulnerabilities should update the firmware immediately from the Linksys website to prevent potential risks.

See more:

1. Restart the router and modem properly?
2. The router is not as safe as you think
3. How to detect VPNFilter malware before it destroys the router
4. Warning, the botnet campaign called GhostDNS is taking over more than 100000 routers