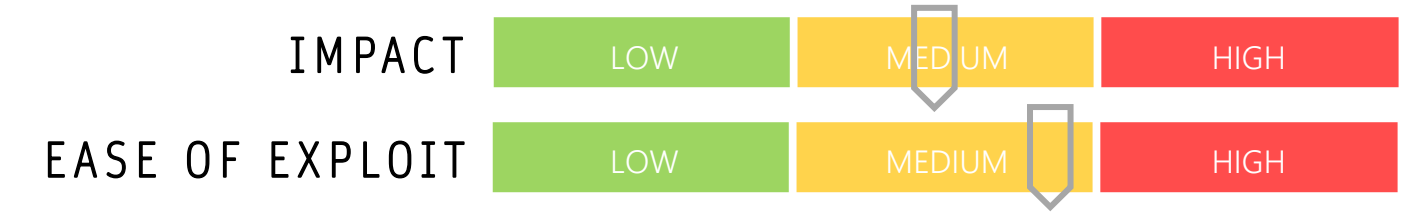
UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00013

CISCO VPN ROUTER VULNERABILITIES

DATE ISSUED: 18th July 2020



OVERVIEW

34 vulnerabilities have been announced in relation to Cisco routers, five of which are noted as being critical.

BREAKDOWN

The Cisco series for small business such as the RV110W Wireless-N VPN Firewall routers have a security flaw relating to the Telnet service due to a default, set password. The RV110W, RV130, RV130W, and RV215W routers also have a flaw by which malicious HTTP requests are created to exploit the improper validation problems and the ability to bypass authentication present in the online management portal. Authentication issues present in the web and hardware management interfaces may result in unauthorised privileged access and the execution of arbitrary code. The hardware interface in particular may be susceptible to abuse in relation to how user input is handled. Likewise, the Cisco Prime License Manager (PLM) suffers similar user input issues however in this case, as attacker is required to have a valid set of login credentials.

REMEDIATION STEPS

- Accept updates prompted by devices or manually install latest round of updates to all affected router and firewall appliances.

REFERENCES & RESOURCES

ZDNet: https://www.zdnet.com/article/cisco-releases-fixes-for-critical-vpn-router-vulnerabilities/
CIS: https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-cisco-products-could-allow-for-arbitrary-code-execution_2020-097/
Cisco: https://www.cisco.com/c/en/us/support/routers/small-business-rv-series-routers/products-security-advisories-list.html
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190904-sb-vpnrouter