Written by Marco Attard
17 June 2016

Customers using three Cisco VPN firewalls and routers from the SMB RV series should be warned the devices carry a critical vulnerability hackers can exploit to remotely take control of devices, if not entire systems.

The vulnerability involves the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, RV130W Wireless-N Multifunction VPN Router and RV215W Wireless-N VPN Router. If the devices are configured for remote management attackers can send an unauthenticated HTTP request with custom user data, leading to remote code execution with root-level priviledges on the affected system.

"A successful exploit could allow the attacker to execute arbitrary script in the context of the web-based management interface for the device or allow the attacker to access sensitive browser-based information," a Cisco security advisory reads.

Patches resolving the issues are still not available. Instead, the company says it should release firmware updates to address the flaw sometime during Q3 2016.

As if the situation is not bad enough, Cisco also warns of a medium-severity XXS flaw and and 2 medium-risk buffer overflows potentially resulting in denial-of-service conditions. Triggering the XSS flaw requires tricking authenticated users to click on specific URLs, while attackers need an authenticated session in the device web-based interface to exploit the buffer overflows.

The XSS flaw is particularly bad, since it remains a concern even if users disable remote

management for protection against the critical flaw. Either way, once Cisco issues updates resolving the issues these should be installed on customers' hardware as soon as possible.

Go Cisco RV110W, RV130W, and RV215W Routers Arbitrary Code Execution Vulnerability