Written by Marco Attard
07 March 2014

A number of Cisco WLAN controller products in use by a many SMB customers are susceptible to multiple security threats, leading the company releasing several patches.

The patches fix two critical vulnerabilities-- one to denial-of-service attacks and the other giving attackers "unauthorised priviledged access to the affected device."

Vulnerable devices include the 500 series wireless express mobility controllers, 2000 and 2100 series WLAN controllers and the Cisco Virtual Wireless Controller, among many others.

The news follows the emergence of the so-called "Moon Worm" affecting Linksys-branded consumer and small business routers. According to Cisco the worm "connects to port 8080 and uses the Home Network Administration Protocol (HNAP) to identify the make and firmware of the compromised router. It then exploits a CGI script to access the router without authentication and scan for other vulnerable boxes."

However, to show commitment to security Cisco reveals the Security Grand Challenge-- a "a global, industry-wide initiative to bring the security community together to address securing the Internet of Things (IoT)." The challenge offers up to $300000 in prize money for innovations stopping attacks on IoT devices, and is open to qualified solution providers across the world.

Cisco will evaluate proposals on several criteria, including feasibility, scalability, performance, ease of use, applicability to multiple verticals, technical maturity/viability and proposer expertise.

It all sounds well and good, but is Cisco able to handle the threats brought about with so many devices (from 10 billion today to 50 billion by 2020, Cisco forecasts) online? Either way the deadline to Security Grand Challenge entries is 17 June 2014.

Go Multiple Vulnerabilities in Cisco WLAN Controllers

Go Cisco Security Grand Challenge