Tim Ring

March 07, 2014

Cisco flaws put routers back in the dock

A major flaw in Cisco's routers has been revealed just days after research firm Team Cymru reported it had found over 300,000 other routers infected with malware.

Cisco issued a patch for its vulnerability on 5 March. The problem lies in the web management interface of its leading Cisco RV215W and CVR100W Wireless-N VPN routers, which could allow a remote attacker to take control of them.

Cisco also issued fixes for multiple vulnerabilities in its Wireless LAN Controller (WLC) product family, and a flaw in its RV110W Wireless-N VPN firewall product.

Cisco flaws put routers back in the dock

The patches follow a report last month from the US SANS Institute that it had found the 'Moon' worm infecting Cisco Linksys-branded routers.

Then on 4 March *SCMagazineUK.com* reported that researchers at US-based Team Cymru had uncovered a 'Man in the Middle' attack dating back to at least mid-December which had infected more than 300,000 small office/home office (SOHO) routers from manufacturers including D-Link, Micronet, Tenda, TP-Link and others.

There are no suggestions the Cisco problem and the SOHO router attack are linked, but the incidents have underlined that routers are a major new corporate vulnerability, whether they are inside the network or being used by a partner small businesses or executives working from home.

Steve Santorelli, outreach manager at Team Cymru, said the two cases revealed the same "disturbing" and "fundamental" issue.

He told *SCMagazineUK.com* via email: "Hacking different elements on an enterprise topology is the new 'black', as opposed to infecting the end client or server. It means that vendors and their enterprise customers have yet another thing to keep them up worrying at night: is your router, your appliance, your DNS infrastructure all actually doing what you think it is?

"It makes perfect sense to evolve in this direction, at least from a criminal perspective: it's harder to spot, you get a massive amount of opportunity to gather credentials and usurp traffic and, just by hacking one part of the topology, you get the equivalent of infecting the entire network of end users: you'd have to spend a *huge* amount of additional time to infect an equivalent number of individual computers."

Santorelli added: "If Cisco machines are being targeted, it's likely due to economies of scale: their routers are everywhere so it makes sense to spend your criminal R&D on them as you'll get the most return on Investment."

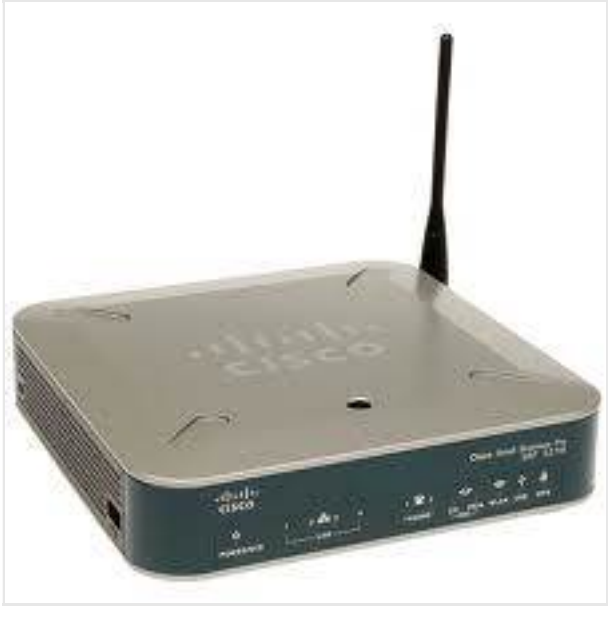
SCMagazineUK.com contacted Cisco for a comment on the issue but they declined. The company did say there are no known workarounds available for its router flaw, but that it was not aware of any malicious use of the vulnerability.

Cisco's security advisory confirmed the problem could allow an attacker to hijack the routers and potentially infiltrate company networks: "The vulnerability is due to improper handling of authentication requests by the web framework. An attacker could exploit this vulnerability by intercepting, modifying and resubmitting an authentication request. Successful exploitation of this vulnerability could allow an unauthenticated, remote attacker to gain administrative-level access to the web management interface of the affected device."

Cisco flaws put routers back in the dock

March 07, 2014

A major flaw in Cisco's routers has been revealed just days after research firm Team Cymru reported it had found over 300,000 other routers infected with malware.



Cisco flaws put routers back in the dock

Cisco issued a patch for its vulnerability on 5 March. The problem lies in the web management interface of its leading Cisco RV215W and CVR100W Wireless-N VPN routers, which could allow a remote attacker to take control of them.

Cisco also issued fixes for multiple vulnerabilities in its Wireless LAN Controller (WLC) product family, and a flaw in its RV110W Wireless-N VPN firewall product.

The patches follow a report last month from the US SANS Institute that it had found the 'Moon' worm infecting Cisco Linksys-branded routers.

Then on 4 March *SCMagazineUK.com* reported that researchers at US-based Team Cymru had uncovered a 'Man in the Middle' attack dating back to at least mid-December which had infected more than 300,000 small office/home office (SOHO) routers from manufacturers including D-Link, Micronet, Tenda, TP-Link and others.

There are no suggestions the Cisco problem and the SOHO router attack are linked, but the incidents have underlined that routers are a major new corporate vulnerability, whether they are inside the network or being used by a partner small businesses or executives working from home.

Steve Santorelli, outreach manager at Team Cymru, said the two cases revealed the same "disturbing" and "fundamental" issue.

He told *SCMagazineUK.com* via email: "Hacking different elements on an enterprise topology is the new 'black', as opposed to infecting the end client or server. It means that vendors and their enterprise customers have yet another thing to keep them up worrying at night: is your router, your appliance, your DNS infrastructure all actually doing what you think it is?

"It makes perfect sense to evolve in this direction, at least from a criminal perspective: it's harder to spot, you get a massive amount of opportunity to gather credentials and usurp traffic and, just by hacking one part of the topology, you get the equivalent of infecting the entire network of end users: you'd have to spend a *huge* amount of additional time to infect an equivalent number of individual computers."

Santorelli added: “If Cisco machines are being targeted, it's likely due to economies of scale: their routers are everywhere so it makes sense to spend your criminal R&D on them as you'll get the most return on Investment.”

SCMagazineUK.com contacted Cisco for a comment on the issue but they declined. The company did say there are no known workarounds available for its router flaw, but that it was not aware of any malicious use of the vulnerability.

Cisco's security advisory confirmed the problem could allow an attacker to hijack the routers and potentially infiltrate company networks: “The vulnerability is due to improper handling of authentication requests by the web framework. An attacker could exploit this vulnerability by intercepting, modifying and resubmitting an authentication request. Successful exploitation of this vulnerability could allow an unauthenticated, remote attacker to gain administrative-level access to the web management interface of the affected device.”