FOSSBYTES

# Critical Bug Allows CIA To Control 318 Cisco Switch Models, No Fix Available

*Cisco suggests disabling telnet for incoming connections.*

By Adarsh Verma

March 21, 2017

*Short Bytes: A vulnerability has been spotted in Cisco's Cluster Management Protocol (CMP) which exposes 318 Cisco Switch models to malicious attacks comprising full control of the device. The flaw arises out of the inability to restrict the use of CMP-specific telnet protocol for local communications. Cisco has suggested some measures for reducing the attack chances before they push the software update for the device.*

The Vault 7 revelation by Wikileaks brought to light the plethora of vulnerabilities in various devices that the CIA can leverage while performing hacking activities. Various companies including Apple and Google confirmed that they've fixed the bugs exposed in the CIA data leak. But it appears the dark clouds are still over the roofs of Cisco Systems.

The researchers at Cisco have found a critical vulnerability (CVE-2017-3881) in more than 300 models of their switches. The bug can allow potential hackers and agencies like CIA to take full control of the switches remotely.

According to an advisory, the bug rests on the Cisco Cluster Management Protocol (CMP) and allows an attacker to perform remote code execution with elevated privileges. CMP uses the telnet protocol as a means of signaling and sending commands on internal networks.

Cisco says the vulnerability arises out of the failure to limit the use of telnet options for local communications between clusters. Also, due to the incorrect processing of malformed CMP-specific telnet options.

To take advantage of the vulnerability, an attacker can send “malformed CMP-specific telnet options while establishing a telnet session with an affected Cisco device configured to accept telnet connections.”

“An exploit could allow an attacker to execute arbitrary code and obtain full control of the device or cause a reload of the affected device.”

According to the advisory, there is “no workaround for the vulnerability, ” and the company will be pushing software updates in the future. However, it only exists when the affected device is configured to accept incoming telnet connections. So, as a countermeasure, Cisco suggests disabling telnet for incoming connections with the help of the following instructions. The use of SSH protocol has been recommended.

The users who don’t want to disable telnet can reduce the threat intensity by implementing infrastructure access control lists, putting a check on the devices that are authorized to send/receive telnet commands.

If you have something to add, drop your thoughts and feedback.

Republished for educational purposes only.