CERT-EU Security Advisory 2017-006

Critical Cisco CMP Remote Code Execution Vulnerability

May 11, 2017 — v1.1

History:

- *21/03/2017 — v1.0: Initial publication*
- *11/05/2017 — v1.1: Software update available from CISCO*

Summary

On March 7th, 2017, Wikileaks made public a set of documents that is being referred to as the *Vault 7 leak*. Based on the *Vault 7* data, Cisco launched an investigation [2] into the products that could potentially be impacted by these and similar exploits and vulnerabilities. As part of the internal investigation of their products and the publicly available information, Cisco security researchers found a vulnerability [1, 5] in the Cluster Management Protocol (CMP) code in Cisco IOS and Cisco IOS XE software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or remotely execute code with elevated privileges.

Cisco has now released a software fix for this vulnerability.

Technical Details

The Cluster Management Protocol (CMP) utilizes internally **telnet** as a signaling and command protocol between cluster members. CMP/IP is the transport mechanism to exchange management packets between the command switch and member switches. The vulnerability is due to the combination of two factors:

- the failure to restrict the use of CMP-specific telnet options only to internal, local communications between cluster members, and instead accept and process such options over any telnet connection to an affected device, and
- the incorrect processing of malformed CMP-specific telnet options.

An attacker could exploit this vulnerability by sending 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.

Products Affected

The vulnerability affects:

- Catalyst switches,
- Embedded Service 2020 switches,
- Enhanced Layer 2 EtherSwitch Service Module,
- Enhanced Layer 2/3 EtherSwitch Service Module,
- Gigabit Ethernet Switch Module (CGESM) for HP,
- IE Industrial Ethernet switches,
- ME 4924-10GE switch, RF Gateway 10,
- SM-X Layer 2/3 EtherSwitch Service Module

An extensive list (300+) of affected devices[1] can be found in [1].

The vulnerability affects Cisco devices running Cisco IOS and IOS XE. Cisco devices running a vulnerable Cisco IOS XE release are affected by this vulnerability when the following conditions are met:

- the CMP subsystem is present on the Cisco IOS XE software image running on the device,
- the device is configured to accept incoming telnet connections.

In Cisco IOS XE, in order to determine if the CMP subsystem is present on the running software image, execute the command `show subsys class protocol | include ^cmp` from a privileged CLI prompt on the device.

The following example shows the output of this command when the CMP subsystem is present on the software image running on the device:

```
#show subsys class protocol | include ^cmp
cmp                                Protocol    1.000.001
```

If the output of the command is empty then CMP subsystem is **not** present on the running software image.

In order to determine if the device is configured to accept incoming telnet connections, execute the command `show running-config | include ^line vty|transport input` from a privileged CLI prompt.

Be sure that the `transport input` configuration line after the line `vty` configuration line is present and configured to only accept the Secure Shell (SSH) protocol for incoming connections to **all** the available VTYs like the example below:

```
#show running-config | include ^line vty|transport input
line vty 0 4
 transport input ssh
line vty 5 15
 transport input ssh
```

[1] Considering the number of affected devices reported by Cisco in [1], it is envisagable that other older – no longer officially supported devices – may also be affected by this vulnerability, so the list may be not-exhaustive.

The following configuration lines show examples of a vulnerable software version:

```
line vty 6 15

line vty 0 4
 transport input all
line vty 0 4
     transport input ssh
line vty 5
 transport input ssh
line vty 6 15 (default=vulnerable)
```

Recommendations

Cisco has released software updates that address this vulnerability [1].

Additionally, as a mitigation to this vulnerability, follow Cisco best practices replacing the **telnet** protocol with the **SSH** protocol as an allowed protocol for incoming connections, thus eliminating the exploit vector. Information on how to implement it can be found on the Cisco Guide to Harden Cisco IOS Devices [3]. In case the SSH protocol is not available in the specific IOS version used, upgrade the IOS version to one that supports it.

In case SSH cannot be used and telnet has to be allowed, a measure that can reduce the attack surface is to implement Infrastructure Access Control Lists (iACLs). Information on iACLs can be found on the following Cisco document: *Protecting Your Core: Infrastructure Protection Access Control Lists* [4].

Cisco IPS Signature 7880-0 and Snort SIDs 41909 and 41910 can also be used to detect attempts to exploit this vulnerability.

NOTE: *Since only limited amount of information is available with regard to this vulnerability and no specific details of the software update is provided, it is strongly recommended to monitor the network traffic using the above mentioned Cisco IPS signature and Snort rules.*

Finally, it is important to realize that even after a patch is published by Cisco, it is useful to re-assess the need to use the CMP. It appears that the CMP will always use telnet for remote management. Given that there is no separation of the *control* and the *data* plane in a lot of switches (that eventually changes with the new models), it is advisable to avoid clustering altogether.

References

[1] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170317-cmp

[2] https://blogs.cisco.com/security/the-wikileaks-vault-7-leak-what-we-know-so-far

[3] https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html

[4] https://www.cisco.com/c/en/us/support/docs/ip/access-lists/43920-iacl.html

[5] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3881