CERT-EU Security Advisory 2017-015

Cisco SNMP Remote Code Execution Vulnerabilities

June 30, 2017 — v1.0

History:

- *30/06/2017 — v1.0: Initial publication*

Summary

The Simple Network Management Protocol (SNMP) subsystem of Cisco IOS and IOS XE Software contains multiple vulnerabilities that could allow **an authenticated**, attacker to **remotely execute code** on an affected system or cause an affected system to reload [1]. An attacker could exploit these vulnerabilities by sending a crafted SNMP packet to an affected system via IPv4 or IPv6.

There are currently no patches available to fix this vulnerability, but Cisco is planning to release them [1]. Workarounds allowing to mitigate the risk are available.

Technical Details

The vulnerabilities are due to a buffer overflow condition in the SNMP subsystem of the affected software. The vulnerabilities affect all versions of SNMP - Versions 1, 2c, and 3. To exploit these vulnerabilities via **SNMP Version 2c or earlier**, the attacker must know the SNMP **read-only community string** for the affected system. To exploit these vulnerabilities via **SNMP Version 3**, the attacker must have **user credentials** for the affected system.

A successful exploit could allow the attacker to **execute arbitrary code** and obtain full control of the affected system or cause the affected system to reload. Exploitation of these vulnerabilities will cause an affected device to reload and generate a `crashinfo` file. In case this file is found, contact the Cisco Technical Assistance Center (TAC) to review the file and determine whether the device has been compromised by exploitation of these vulnerabilities.

Cisco is aware of external knowledge of these vulnerabilities, so there is the potential for exploitation [1].

Products Affected

These vulnerabilities affect all releases of Cisco IOS and IOS XE Software prior to the first fixed release, and they affect all versions of SNMP—Versions 1, 2c, and 3.

Devices configured with any of the following MIBs are vulnerable:

```
ADSL-LINE-MIB
ALPS-MIB
CISCO-ADSL-DMT-LINE-MIB
CISCO-BSTUN-MIB
CISCO-MAC-AUTH-BYPASS-MIB
CISCO-SLB-EXT-MIB
CISCO-VOICE-DNIS-MIB
CISCO-VOICE-NUMBER-EXPANSION-MIB
TN3270E-RT-MIB
```

Although the `show snmp mib` command can be used to display a list of the MIB OIDs that are registered on a system, use of a network management system (NMS) application is the recommended solution for gathering this information [1].

Recommendations

No fixes are available at this time. When fixes will become available, they will be available as new software versions for the customers who have valid license, through the regular update channels [1].

Workarounds

Administrators are advised to allow only trusted users to have SNMP access on an affected system. Administrators are also advised to monitor affected systems by using the `show snmp host` command in the CLI. In addition, administrators can mitigate these vulnerabilities by disabling the MIBs listed in the previous section [1].

To help customers determine their exposure to vulnerabilities in Cisco IOS and IOS XE Software, Cisco provides a tool, the Cisco IOS Software Checker [2] that identifies any Cisco Security Advisories that impact a specific software release and the earliest release that fixes the vulnerabilities described in each advisory (*First Fixed*). If applicable, the tool also returns the earliest release that fixes all the vulnerabilities described in all the advisories identified (*Combined First Fixed*).

References

[1] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170629-snmp

[2] https://tools.cisco.com/security/center/selectIOSVersion.x