Security Advisory 2019-012

Thrangrycat – Critical Vulnerability Affecting Most Cisco Devices

May 14, 2019 — v1.0

TLP:WHITE

History:

- *14/05/2019 — v1.0 – Initial publication*

Summary

Cisco Secure Boot helps to ensure that the code that executes on Cisco hardware platforms is authentic and unmodified [1]. The Cisco Secure Boot Hardware Tampering vulnerability (CVE-2019-1649) could allow an authenticated, local attacker to write a modified firmware image to the component. A successful exploit could either cause the device to become unusable (and require a hardware replacement) or allow tampering with the Secure Boot verification process [2]. When abused together with Cisco IOS XE Software Web UI Command Injection Vulnerability [5], it may be possible to attack also from a remote network [4].

Technical Details

The Cisco Secure Boot Hardware Tampering vulnerability is due to an improper check on the area of code that manages on-premise updates to a Field Programmable Gate Array (FPGA) part of the Secure Boot hardware implementation. An attacker with elevated privileges and access to the underlying operating system that is running on the affected device could exploit this vulnerability by writing a modified firmware image to the FPGA. A successful exploit could either cause the device to become unusable (and require a hardware replacement) or allow tampering with the Secure Boot verification process, which under some circumstances may allow the attacker to install and boot a malicious software image.

An attacker will need to fulfill all the following conditions to attempt to exploit this vulnerability:

- Have privileged administrative access to the device.
- Be able to access the underlying operating system running on the device; this can be achieved either by using a supported, documented mechanism or by exploiting another vulnerability (such as for instance Cisco IOS XE Software Web UI Command Injection Vulnerability [5]) that would provide an attacker with such access.
- Develop or have access to a platform-specific exploit. An attacker attempting to exploit this vulnerability across multiple affected platforms would need to research each one of

those platforms and then develop a platform-specific exploit. Although the research process could be reused across different platforms, an exploit developed for a given hardware platform is unlikely to work on a different hardware platform.

Products Affected

Cisco has investigated all Cisco products that support hardware-based Secure Boot functionality to verify that they are enforcing the appropriate access control checks.

Only products listed in the Vulnerable Products section of [2] are known to be affected by this vulnerability.

Recommendations

Cisco will release software updates that address this vulnerability. There are no workarounds that address this vulnerability.

Cisco provides information about how to harden the device and secure management access in [3]. Implementing the recommendations in this document would reduce the attack surface for this vulnerability.

References

[1] https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/trustworthy-technologies-datasheet.pdf

[2] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190513-secureboot

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

[4] https://thrangrycat.com/

[5] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190513-webui