1700 - Cisco Catalyst Exploitation

Friday at 17:00 in 101 Track
45 minutes | Demo
Artem Kondratenko*Penetration Tester, Security Researcher*

On March 17th, Cisco Systems Inc. made a public announcement that over 300 of the switches it manufactures are prone to a critical vulnerability that allows a potential attacker to take full control of the network equipment.

This damaging public announcement was preceded by Wikileaks' publication of documents codenamed as "Vault 7" which contained information on vulnerabilities and description of tools needed to access phones, network equipment and even IOT devices.

Cisco Systems Inc. had a huge task in front of them - patching this vast amount of different switch models is not an easy task. The remediation for this vulnerability was available with the initial advisory and patched versions of IOS software were announced on May 8th 2017.

We all heard about modern exploit mitigation techniques such as Data Execution Prevention, Layout Randomization. But just how hardened is the network equipment? And how hard is it to find critical vulnerabilities?

To answer that question I decided to reproduce the steps necessary to create a fully working tool to get remote code execution on Cisco switches mentioned in the public announcement.

This presentation is a detailed write-up of the exploit development process for the vulnerability in Cisco Cluster Management Protocol that allows a full takeover of the device.
Artem Kondratenko
Artem is a Penetration Tester at Kaspersky Lab. On time between red team engagements he is doing security research of software and hardware appliances. Author of multiple CVE's on VMware Virtualization Platforms (CVE-2016-5331, CVE-2016-7458, CVE-2016-7459, CVE-2016-7460). Enjoys contributing to the community by writing penetration testing tools such as Invoke-Vnc (PowerShell vnc injector, part of CrackMapExec) and Rpivot (reverse socks4 proxy, now part of BlackArch Linux Distro).

@artkond, https://github.com/artkond,
https://artkond.com

#defcon25/by_track/101/Friday #defcon25/By_Day/_Friday