Cyberint
Protection Beyond the Perimeter

Security Bulletin

Cisco Smart Install (SMI)

www.cyberint.com

Cyberint
Protection Beyond the Perimeter

Contents

Introduction

Over the past forty-eight hours, since 5 April 2018, there have been numerous open source reports of wide spread cyberattacks targeting Cisco networking devices, specifically switches using the Cisco Smart Install Client, primarily within Iran and Russia.

Cisco Talos[1] Intelligence Group reports that multiple organisations, including those operating critical infrastructure, have been targeted worldwide by a protocol misuse issue within the Cisco Smart Install Client, a utility designed to allow zero-touch configuration of Cisco Switches.

Whilst the Cisco Talos report ascertains that these attacks may be associated with nation-state threat actors, other reports link and attribute the attacks to the Russian nexus nation-state threat actor known as Dragonfly, potentially due to the 15 March 2018 alert published by US-CERT[2] that detailed attacks against energy, nuclear and commercial facilities.

Aside from the US-CERT report, the security vendor Embedi published a blog post on 29 March 2018 describing a critical Stack Buffer-Overflow Remote Code Execution (RCE) vulnerability, CVE- 2018-0171, within the same Cisco Smart Install Client that "*enables an attacker to remotely execute arbitrary code without authentication*" and "*allows getting full control over vulnerable network equipment*"[3].

Cisco Smart Install (SMI)

Cisco Smart Install allows organisations to deploy new network switches to locations without the need for preconfiguration. Using plug-and-play configuration and image management features, the the smart install devices enable zero-touch deployment by communicating with a common layer-3 switch or router that is acting as a 'director.' This director then, provides a single management point, to deploy configurations or device 'images'. When deploying a new Cisco switch with Smart Install technology, the director detects the device, identifies the appropriate Cisco IOS software image and configuration file before downloading these to the

[1] http://blog.talosintelligence.com/2018/04/critical-infrastructure-at-risk.html
[2] https://www.us-cert.gov/ncas/alerts/TA18-074A
[3] https://embedi.com/blog/cisco-smart-install-remote-code-execution/

device. Furthermore, the director is able to perform on-demand deployments of software images and configurations to individual or groups of Cisco switches within the managed network.

In addition to earlier reported vulnerabilities, organisations that fail to disable or securely configure the SMI protocol can allow threat actors to abuse functionalities such as:

- Modifying TFTP server settings to exfiltrate device configuration files, potentially revealing device secrets or passwords;
- Modification of device configuration, potentially resulting in availability (denial of service) or confidentiality (for example, enabling port-mirroring 'SPAN' to capture network traffic) issues;
- Replacement of the device's IOS image, potentially allowing a compromised device operating system to be deployed;
- Addition and configuration of new user accounts permitting administrative access along with command execution;

Recent Developments

Over the past few days, numerous reports regarding exploitation of these Cisco Smart Client protocol vulnerabilities or flaws have been made public, including attacks against media and communications organisations within Iran and Russia.

Amongst these, major Russian online media providers such as Fontanka.ru[4] and Komsomolskaya Pravda[5] reportedly suffered outages, while 'important' Iranian services and websites where inaccessible due to problems at ISPs in the region[6].

The threat actor behind these attacks is believed to have exploited a misconfiguration of the Cisco Smart Install protocol to override deployed Cisco IOS images or configurations on vulnerable devices, changing them to display seemingly

[4] http://www.fontanka.ru/2018/04/06/130/
[5] https://t.me/truekpru/4566
[6] http://ifpnews.com/exclusive/iranian-databases-target-of-attacks-caused-by-cisco-switch-flaw/

pro-American messages protesting alleged interference in the presidential elections (Figure 1).

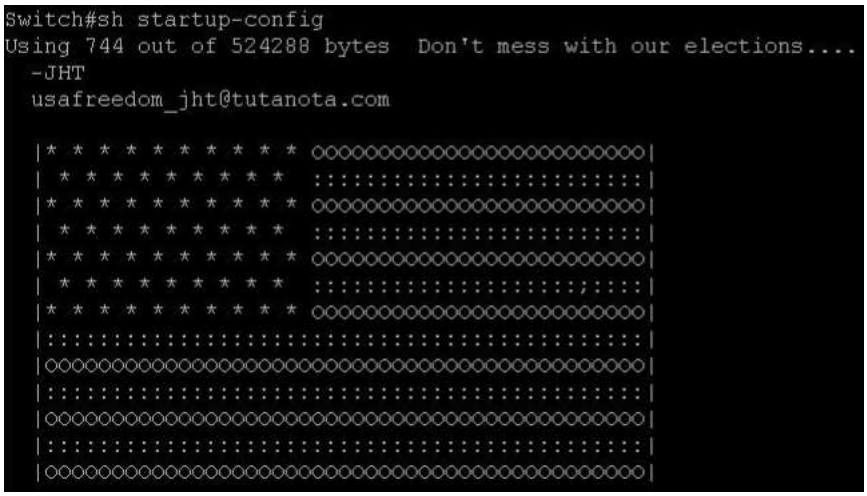

Figure 1 - Compromised Cisco Switch

Given the widespread use of Cisco networking devices within the infrastructure of organisations worldwide, the threat from this vulnerability is widespread. A Shodan search for Cisco devices exposing the Smart Install Client protocol revealed over 168,000 internet-accessible devices (Figure 2).

Figure 2 – Cisco Smart Install Client Exposure (Shodan.io)

Scans for SMI-enabled devices (port 4786) have started in February 2017, intensified in October, and doubled after the last Cisco Talos warning in February, this year.

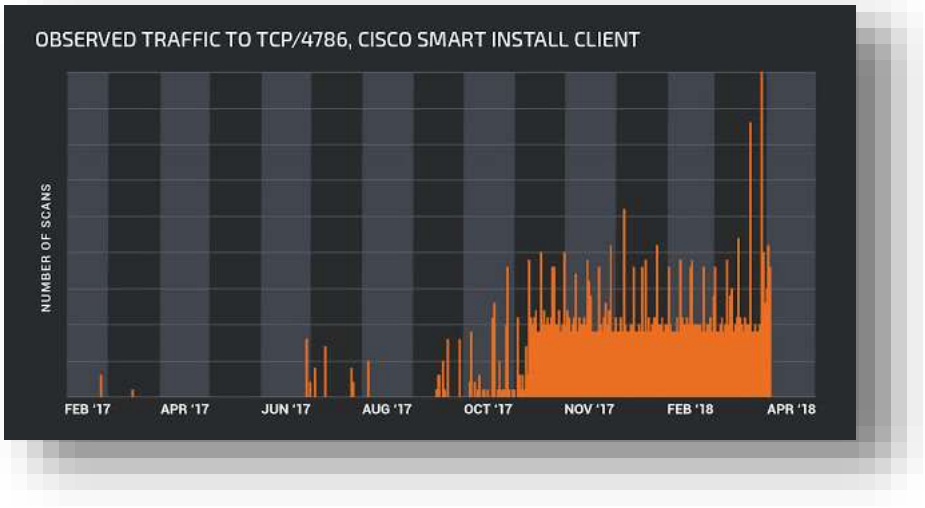

Figure 3 - Observerd Traffic to tcp 4786, cisco smart install client

The misuse of this Cisco IOS smart install feature was first reported by Cisco in February 2017[7], with scans for SMI-enabled devices intensifying in October 2017, prompting the release of a configuration guide that details how to disable or harden IOS devices against misuse of protocol, last updated on 26 March 2018[8]. Furthermore, Cisco Talos have released an open source tool to scan networks to determine if there are any Smart Install enabled devices present[9].

Conclusions

Whilst the Cisco Talos report links to the recent US-CERT publication attributing attacks to the Russian nexus nation state threat actor known as Dragonfly, it is understood that the recent remote code execution vulnerability, CVE-2018-0171 published by Embedi is not related to this incident[10].

[7] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170214-smi
[8]https://www.cisco.com/c/en/us/td/docs/switches/lan/smart_install/configuration/guide/smart_install/concepts.html
[9] https://github.com/Cisco-Talos/smi_check
[10]https://www.bleepingcomputer.com/news/security/cyber-attacks-on-us-critical-infrastructure-linked-to-cisco-switch-flaw/

Furthermore, given the seemingly pro-American sentiment and the reported location of exploited devices, we assess with moderate confidence that these recent events are not related or attributed to any known threat actor. Based on the tactics, techniques and procedures (TTP) observed, combined with the victim geolocation and detail reported thus far, we believe that these incidents are currently unrelated to previous Dragonfly operations.

Recommendations

- Using the Cisco Talos published utility[11], or another method to detect Cisco SMI-enabled switches operating on port 4786, organisations should scan their network infrastructure for any potentially vulnerable devices;
- Cisco best-practice and device hardening guides should be followed to ensure that any deployed device is suitably secured and Smart Install is suitably protected or disabled;
- Where applicable, patch Cisco IOS devices with Smart Install against the vulnerability detailed in CVE-2018-0171;

[11] https://github.com/Cisco-Talos/smi_check