REDSEAL SOLUTION NOTE

ALERT: CISCO REST API CONTAINER FOR IOS XE AUTHENTICATION BYPASS VULNERABILITY

RELEASE DATE: NOVEMBER 2019

DESCRIPTION OF ALERT

Cisco announced an authentication bypass vulnerability in the REST API virtual service container for IOS XE Software allowing an unauthenticated attacker to access the router by submitting malicious HTTP requests to the targeted device. This is being tracked with CVE-2019-12643.

This vulnerability can lead to configuration modification, loss of network segmentation, sensitive data release and service disruption.

Security and network managers are faced with the difficulty of identifying all potentially vulnerable devices on their network and applying mitigating controls and remediation in a timely manner.

AFFECTED PRODUCTS

Cisco 4000 Series Integrated Services Routers

Cisco ASR 1000 Series Aggregation Services Routers

Cisco Cloud Services Router 1000V Series

Cisco Integrated Services Virtual Router

(ONLY if the device runs an affected IOS XE Software Release AND the device has an installed and enabled affected version of the Cisco REST API virtual service container)

VENDOR SOLUTION

Upgrade the Cisco REST API virtual service container to a fixed release.

REDSEAL RECOMMENDED ACTIONS

RedSeal can detect OS and patch version numbers for Cisco assets and provide a quick inventory report for assets that require mitigation. Additional identification can be verified using RedSeal's custom best practice checks to identify affected devices.

REDSEAL RECOMMENDS THAT CUSTOMERS USE REDSEAL TO

a) Create an inventory of their Cisco devices

b) Run a custom best practice check to receive a list of vulnerable devices

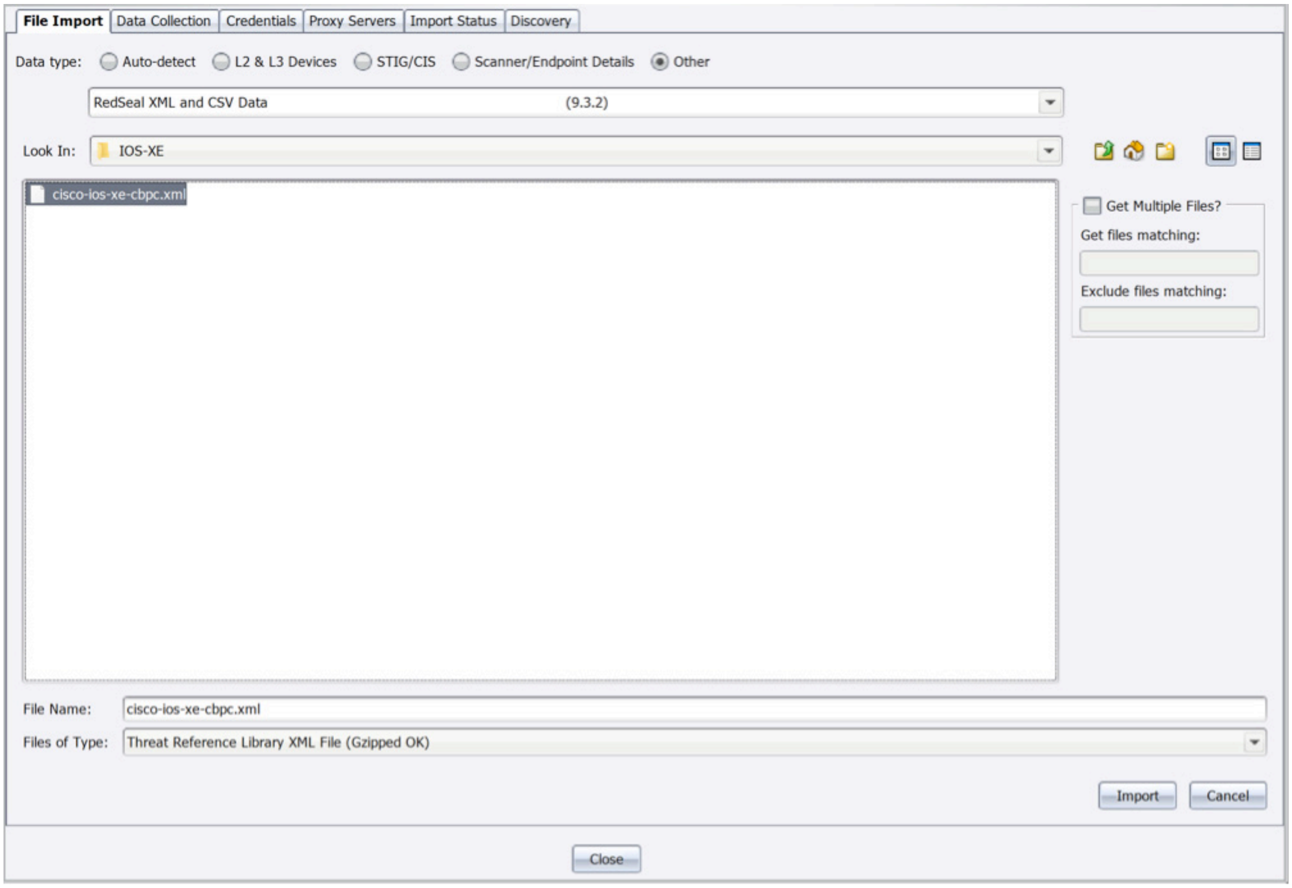
c) Create and run daily reports until all affected systems are patched

ALERT AT A GLANCE

1. A high impact vulnerability that impacts Cisco IOS XE REST API functionality was announced
2. Vulnerability could allow unauthorized access to routers
3. A RedSeal inventory report can quickly provide information to identify affected systems
4. A RedSeal custom best practice check can further identify affected systems
5. Create and run daily reports until all affected systems are patched

DIRECTIONS TO DOWNLOAD AND IMPORT CUSTOM BEST PRACTICE CHECK

1. Navigate and login in to RedSeal Customer Support Portal located at https://www.redseal.net/services/#customer-support
2. On landing page scroll down to the message titled Cisco REST API Container for IOS XE Authentication Bypass Vulnerability Check.
3. Download Custom Best Practice Check .xml File via the webpage under the message for this alert. (File Name: cisco-ios-xe-cbpc.xml)
4. After downloading the file, log into RedSeal and Import the file as Other -> RedSeal XML and CSV.



Data type: ○ Auto-detect ○ L2 & L3 Devices ○ STIG/CIS ○ Scanner/Endpoint Details ● Other

RedSeal XML and CSV Data (9.3.2)

Look In: IOS-XE

cisco-ios-xe-cbpc.xml

□ Get Multiple Files?

Get files matching:

Exclude files matching:

File Name: cisco-ios-xe-cbpc.xml

Files of Type: Threat Reference Library XML File (Gzipped OK)

5. After import, custom best practice check will be available.

REFERENCES

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190828-iosxe-rest-auth-bypass#vp

https://www.redseal.net/using-redseal-to-fix-cracks-in-the-foundation/