REDSEAL SOLUTION NOTE

REDSEAL

ALERT: FORTINET PATH TRAVERSAL VULNERABILITY CHECK

RELEASE DATE: 21 OCTOBER 2019

DESCRIPTION OF ALERT

Fortinet announced a path traversal vulnerability in the FortiOS SSL VPN web portal that may enable an unauthenticated attacker to download FortiOS system files through specially crafted HTTP resource requests. This is being tracked with the following CVEs; CVE-2018-13379 & CVE-2018-13383.

This vulnerability can lead to a loss of security credentials that are a prelude to data leaks. Sensitive data release can potentially negatively impact a company's reputation and expose it to millions of dollars in fines.

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

FortiOS 6.0 - 6.0.0 to 6.0.4

FortiOS 5.6 - 5.6.3 to 5.6.7

FortiOS 5.4 - 5.4.6 to 5.4.12

ONLY if the SSL VPN service (web-mode or tunnel-mode) is enabled. (other branches and versions than above are not impacted)

VENDOR SOLUTION

Upgrade to FortiOS 5.6.8 or above, 6.0.5 or above, 6.2.0 or above, or upcoming 5.4.13.

REDSEAL RECOMMENDED ACTIONS

RedSeal can detect OS and patch version numbers for Fortinet assets and provide a quick inventory report for Fortinet assets that require mitigation. Additional identification can be verified leveraging a RedSeal custom best practice check to identify affected devices.

REDSEAL RECOMMENDS THAT CUSTOMERS USE REDSEAL TO

a) create an inventory of their Fortinet devices,

b) run a custom best practice check to receive a list of vulnerable devices, and

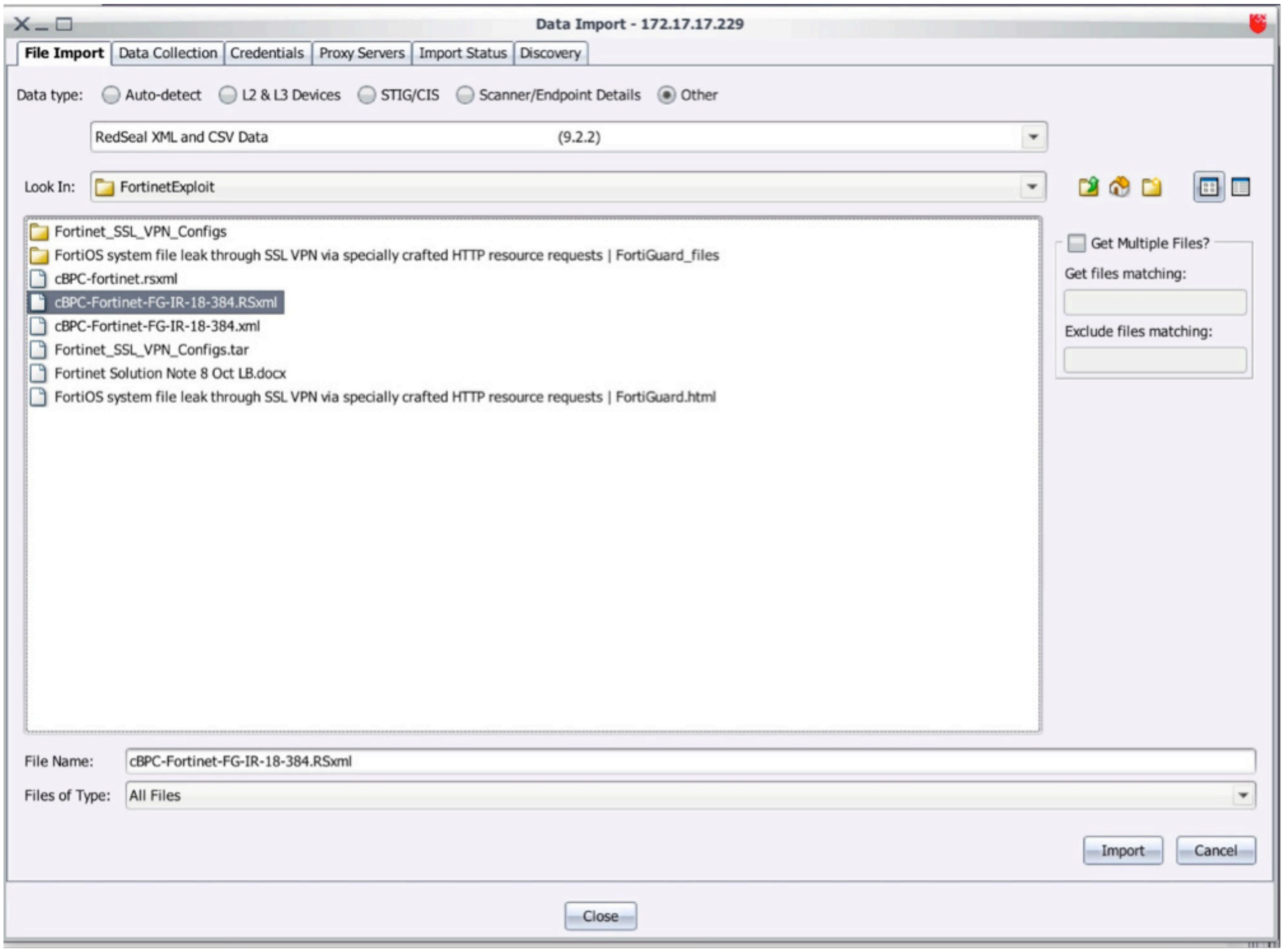
c) create and run daily reports until all affected systems are patched.

ALERT AT A GLANCE

1. A high impact vulnerability that impacts Fortinet SSL functionality was announced
2. Vulnerability could disclose security credentials
3. A RedSeal inventory report can quickly provide information to identify affected systems
4. A RedSeal custom best practice check can 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 Fortinet Path Traversal Vulnerability Check.
3. Download custom best practice check .RSxml File via the webpage under the message for this alert. (File Name: cBPC-Fortinet-FG-IR-18-384.RSxml)
4. After downloading the file, log into RedSeal and import the file as Other -> RedSeal XML and CSV.



Data Import - 172.17.17.229

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

RedSeal XML and CSV Data (9.2.2)

Look In: FortinetExploit

Fortinet_SSL_VPN_Configs
FortiOS system file leak through SSL VPN via specially crafted HTTP resource requests | FortiGuard_files
cBPC-fortinet.rsxml
cBPC-Fortinet-FG-IR-18-384.RSxml
cBPC-Fortinet-FG-IR-18-384.xml
Fortinet_SSL_VPN_Configs.tar
Fortinet Solution Note 8 Oct LB.docx
FortiOS system file leak through SSL VPN via specially crafted HTTP resource requests | FortiGuard.html

□ Get Multiple Files?
Get files matching:
Exclude files matching:

File Name: cBPC-Fortinet-FG-IR-18-384.RSxml
Files of Type: All Files

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

REFERENCES

https://fortiguard.com/psirt/FG-IR-18-384

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