NATIONAL SECURITY AGENCY
CYBERSECURITY ADVISORY

CISCO UPDATES CRITICAL REMOTE CODE EXECUTION VULNERABILITY ADVISORY FOR ASA

DISCUSSION

Cisco® recently updated a vulnerability advisory affecting Cisco Adaptive Security Appliance (ASA) and Firepower®[1] Appliance[2], CVE[3]-2018-0101. The updated release informed users that devices continue to be vulnerable after the 29 January 2018 advisory and software release. Furthermore, Cisco disclosed the existence of additional vulnerable features. The updated advisory, released 5 February 2018, recommends users again install updated software since the versions released on 29 January 2018 do not include fixes for the newly disclosed vulnerabilities.

Below is a consolidated list of affected products and features. Refer to Cisco Security Center for a complete list of vulnerable products and configurations.[4]

- 3000 Series Industrial Security Appliance (ISA)
- ASA 5500 Series Adaptive Security Appliances
- ASA 5500-X Series Next-Generation Firewalls
- ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers
- ASA 1000V Cloud Firewall
- Adaptive Security Virtual Appliance (ASAv)
- Firepower 2100 Series Security Appliance
- Firepower 4110 Security Appliance
- Firepower 4120 Security Appliance
- Firepower 4140 Security Appliance
- Firepower 4150 Security Appliance
- Firepower 9300 ASA Security Module
- Firepower Threat Defense Software (FTD)
- FTD Virtual

This announcement relates to and contains updated information regarding IAVA 2018-A-0042 Cisco Adaptive Security Appliance (ASA) Remote Code Execution Vulnerability released 01 February 2018.

MITIGATION ACTIONS

The only effective mitigating action is to update Cisco software to the latest version by visiting the Cisco Software Center4F5. The Cisco advisory contains an incomplete workaround that addresses a single vulnerable feature by restricting management access of the security appliance to known and trusted hosts. The workaround does not fully mitigate the vulnerability and leaves customers vulnerable to the attack vectors affecting the various other vulnerable features.

---

[1] Cisco and Firepower are registered trademarks of Cisco Systems, Inc.

[2] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180129-asa1#fixed

[3] CVE is a registered trademark of the MITRE Corporation

[4] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180129-asa1#fixed

[5] https://software.cisco.com/download/navigator.html

Customers using Cisco ASA Software prior to release 9.1 as well as the affect 9.3 and 9.5 are recommended to migrate to a supported and unaffected release. Customers using Cisco ASA release 9.3 are recommended to migrate to version 9.4.4.16. Customers using Cisco ASA release 9.5 are recommended to migrate to version 9.6.4.3.

Temporary hotfixes are available from Cisco for customers utilizing the affected Cisco FTD versions, however it is highly recommended to update software to the latest versions. See below for more information.

Cisco FTD major Release	First Fixed Release
6.0.0	Affected; migrate to 6.0.1 Hotfix or later
6.0.1	Cisco_FTD_Hotfix_BH-6.0.1.5-1.sh (All FTD hardware platforms except 41xx and 9300) Cisco_FTD_SSP_Hotfix_BH-6.0.1.5-1.sh (41xx and 9300 FTD hardware platform)
6.1.0	Cisco_FTD_Hotfix_DZ-6.1.0.7-1.sh (All FTD hardware platforms except 41xx and 9300) Cisco_FTD_SSP_Hotfix_DZ-6.1.0.7-1.sh (41xx and 9300 FTD hardware platform)
6.2.0	Cisco_FTD_Hotfix_BN-6.2.0.5-3.sh (All FTD hardware platforms except 41xx and 9300) Cisco_FTD_SSP_Hotfix_BN-6.2.0.5-3.sh (41xx and 9300 FTD hardware platform)
6.2.1	Affected; migrate to 6.2.2 Hotfix
6.2.2	Cisco-FTD_SSP_FP2K_Hotfix_AN-6.2.2.2-4.sh.REL.tar (21xx FTD hardware platform) Cisco_FTD_SSP_Hotfix_AO-6.2.2.2-1.sh.REL.tar (41xx and 9300 FTD hardware platform) Cisco_FTD_Hotfix_AO-6.2.2.2-1.sh.REL.tar (All other FTD hardware platforms)

DISCLAIMER OF WARRANTIES AND ENDORSEMENT

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

FOR FURTHER INFORMATION, PLEASE CONTACT

Client Requirements or General Cybersecurity Inquiries
Cybersecurity Requirements Center
410-854-4200
Email: Cybersecurity_Requests@nsa.gov