TLP: WHITE
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER:
2018-014 **- UPDATED**

DATE(S) ISSUED:
01/30/2018
***02/06/2018* - UPDATED**

SUBJECT:
A Vulnerability in Cisco Adaptive Security Appliance Software Could Allow for Remote Code Execution

OVERVIEW:
A vulnerability has been identified in the Secure Sockets Layer (SSL) VPN functionality of the Cisco Adaptive Security Appliance (ASA) Software, which could allow for remote code execution. The Cisco ASA family of products provide network security services such as firewalls, intrusion prevention systems (IPS), endpoint security (anti-x), and VPNs. Successful exploitation of this vulnerability could result in remote code execution in the context of the affected application. Depending on the privileges associated with the application, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

February 06 – UPDATED OVERVIEW:
There are two new issues related to CVE-2018-0101, which affect users who have already applied the patch as well as increasing the number of vulnerable systems and features affected.

- ***Users who applied the previous fixes to mitigate CVE-2018-0101, which could allow for remote code execution, are now reported to be vulnerable to denial of service attacks.***
- ***In addition, more than a dozen additional systems and features have been identified as being vulnerable to CVE-2018-0101. The newly identified features include the Adaptive Security Device Manager (ASDM), AnyConnect IKEv2 Remote Access and SSL VPN, Cisco Security Manager, Clientless SSL VPN, Cut-Through Proxy, Local Certificate Authority, Mobile Device Manager Proxy, Mobile User Security, Proxy Bypass, the REST API, and Security Assertion Markup Language (SAML) Single Sign-on (SSO).***

THREAT INTELLIGENCE:
There are currently no reports of this vulnerability being exploited in the wild.

SYSTEM AFFECTED:

- 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 9300 ASA Security Module
- Firepower Threat Defense Software (FTD)

February 06 – UPDATED SYSTEMS AFFECTED:

- ***Firepower 4120 Security Appliance***
- ***Firepower 4140 Security Appliance***
- ***Firepower 4150 Security Appliance***

- ***FTD Virtual***

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:
A vulnerability has been identified in the Secure Sockets Layer (SSL) VPN functionality of the Cisco Adaptive Security Appliance (ASA) Software, which could allow for remote code execution. This vulnerability occurs when the *webvpn* feature is enabled on an affected Cisco ASA device, and an attempt to double free a region of memory occurs. The vulnerability can be exploited by sending multiple crafted Extensible Markup Language (XML) packets to a Cisco ASA device that has a *webvpn-configured* interface.

Successful exploitation of this vulnerability could result in remote code execution in the context of the affected application. Depending on the privileges associated with the application, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

February 06 – UPDATED TECHNICAL SUMMARY:
Users who applied the previous fixes to mitigate CVE-2018-0101 are now reported to be vulnerable to denial of service attacks. In addition, more than a dozen additional systems and features have been identified as being vulnerable to CVE-2018-0101.

The vulnerability can be exploited by sending multiple crafted Extensible Markup Language (XML) packets to a Cisco ASA device that has one of the vulnerable features enabled. To be vulnerable, the ASA device must have Secure Sockets Layer (SSL) or IKEv2 Remote Access VPN services enabled. Users who applied the previous fixes to mitigate CVE-2018-0101 are now reported to be vulnerable to additional unspecified Denial of Service conditions. Cisco has released a new set of patches to address these vulnerabilities.

RECOMMENDATIONS:
We recommend the following actions be taken:
- Install updates provided by Cisco immediately after appropriate testing.
- Verify no unauthorized system modifications have occurred on system before applying patch.
- Monitor intrusion detection systems for any signs of anomalous activity.
- Unless required, limit external network access to affected products.

REFERENCES:
Cisco:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180129-asa1

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2018-0101

February 6 – UPDATED REFERENCES:
Cisco:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180129-asa1

Securityweek:
http://www.securityweek.com/cisco-reissues-patches-critical-firewall-flaw

24×7 Security Operations Center
Multi-State Information Sharing and Analysis Center (MS-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722