ASA IOS vulnerability Fix Plan

Vulnerability ID: CVE-2018-0101

A vulnerability in the Secure Sockets Layer (SSL) VPN functionality of the Cisco Adaptive Security Appliance (ASA) Software could allow an unauthenticated, remote attacker to cause a reload of the affected system or to remotely execute code. The vulnerability is due to an attempt to double free a region of memory when the WEBVPN feature is enabled on the Cisco ASA device. An attacker could exploit this vulnerability by sending multiple, crafted XML packets to a WEBVPN-configured interface on the affected system. An exploit could allow the attacker to execute arbitrary code and obtain full control of the system, or cause a reload of the affected device. This vulnerability affects Cisco ASA Software that is running on the following Cisco products: 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 (ASA virtual), Firepower 2100 Series Security Appliance, Firepower 4110 Security Appliance, Firepower 9300 ASA Security Module, Firepower Threat Defense Software (FTD). Cisco Bug IDs: CSCvg35618.

CVE-2018-0101漏洞详情

0x00漏洞背景

2018年1月29日，思科公开了旗下ASA防火墙设备的拒绝服务&远程代码执行漏洞（CVE-2018-0101），并在2月期间多次对公开信息进行修改和更新。在思科更新漏洞相关信息期间，该漏洞也有更多信息被披露出来，其中包括漏洞发现者——NCC Group研究人员Cedric Halbronn关于漏洞细节的更多信息和安全研究者根据相关资料完成的PoC代码（拒绝服务部分）。

  从已经公开的资料来看，该漏洞影响多个版本的思科安全产品和软件。同时，受影响的系统需在网络设备端口上开启SSL服务或IKEv2 VPN服务。如果该漏洞被成功利用，将导致远程设备内存破坏，造成设备重启或拒绝服务，甚至允许攻击者在无需用户验证的情况下实现远程代码执行，进而远程控制设备并产生进一步的攻击行为。本文出于探究漏洞技术原理，了解此类网络设备漏洞分析调试方法的目的，从ASA设备解析XML数据包的过程入手，分析该漏洞产生的原因，并将部分技术细节予以呈现。

**0x01  漏洞简要介绍**

1.     漏洞原理

CVE-2018-0101漏洞存在于思科ASA设备的XML解析器处理XML数据包时的分配和释放内存的过程当中，是一个Double Free漏洞，攻击者可以通过发送精心构造的SSL 协议的HTTP XML数据包来完成对受漏洞影响系统的攻击。当漏洞触发时，可导致系统崩溃重载，ASA设备停止接受VPN验证请求，或允许攻击者远程执行代码，获得对系统的控制。

2.     漏洞影响范围和脆弱性配置信息

思科官方在最初的公开信息中声称：多个版本的ASA和下一代防火墙平台受漏洞影响，且受影响设备需要配置启用WebVPN功能，并允许用户访问。由于发现了新的攻击向量，思科官方在2月份数次更新了安全公告，并在更新中将开通SSL VPN的说法引申为“Secure Socket Layer (SSL) services or IKEv2 Remote Access VPN services”。更新后的受漏洞影响设备和软件列表如下所示：

Ø  3000 Series Industrial Security Appliance (ISA)

Ø  ASA 5500 Series Adaptive Security Appliances

Ø  ASA 5500-X Series Next-Generation Firewalls

Ø  ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers

Ø  ASA 1000V Cloud Firewall

Ø  Adaptive Security Virtual Appliance (ASAv)

Ø  Firepower 2100 Series Security Appliance

Ø  Firepower 4110 Security Appliance

Ø  Firepower 4120 Security Appliance

Ø  Firepower 4140 Security Appliance

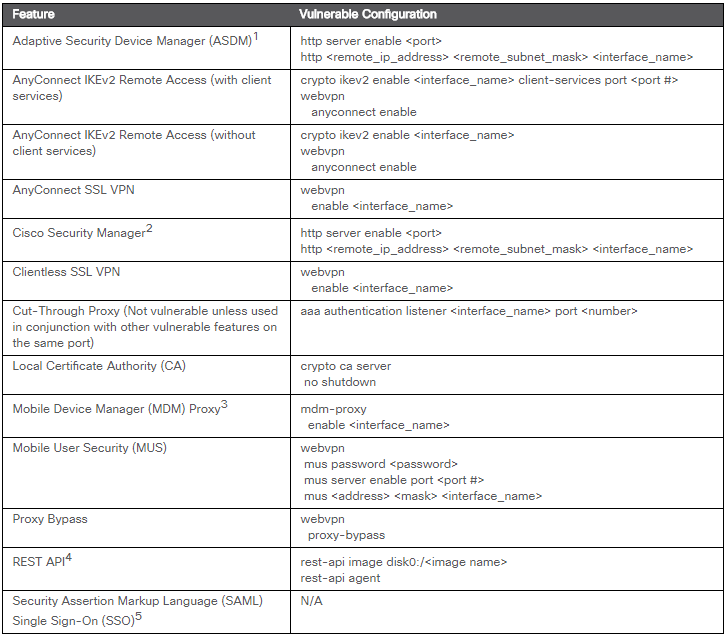
Ø  Firepower 4150 Security Appliance

Ø  Firepower 9300 ASA Security Module

Ø  Firepower Threat Defense Software (FTD)

Ø  FTD Virtual (FTDv)

其中，Cisco ASA中易受攻击的功能列表和配置信息如下所示：

[](https://p2.ssl.qhimg.com/t0174235272e381251f.png)

         在上图的信息中：

1.       ASDM仅受http 命令配置列表范围的IP攻击影响；

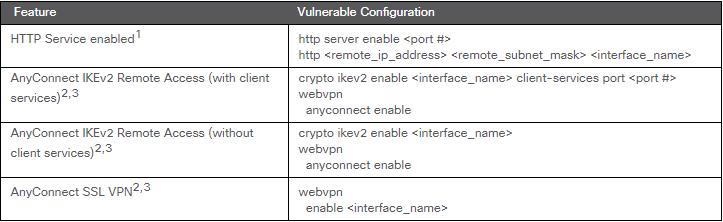
2.       Cisco Security Manager仅受http 命令配置列表范围的IP攻击影响；

3.       MDM 9.3.1以上版本受上述配置影响；

4.       其他API 9.3.2以上版本受上述配置，且仅受http 命令配置列表范围的IP攻击影响；；

5.       SAML SSO 9.6以上版本受上述配置影响。

FTD软件中易受攻击的功能和配置信息如下所示：

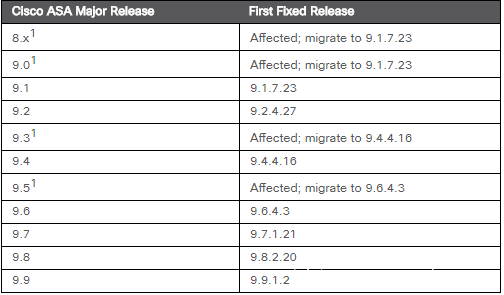
[](https://p5.ssl.qhimg.com/t014f219e93c198ec07.png)

         我们可以看到，上图中的配置信息，均与Web VPN的配置有关。

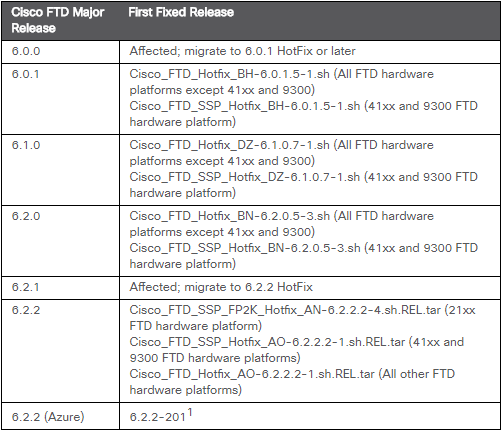
3.     修复方案

由于在1月29日发布报告后发现了新的攻击向量，所以Cisco官方在2月份的后续更新中，对固件升级的版本信息做了变更，细节参见Cisco官方关于CVE-2018-0101的说明。版本升级建议如下：

**Cisco ASA列表：**

[](https://p1.ssl.qhimg.com/t0126fb92d6c0f525b4.png)

**Cisco FTD列表：**

[](https://p2.ssl.qhimg.com/t011114827f957afee8.png)