

安全漏洞通告

【在野利用 | PoC 公开】 CVE-2020-3580: Cisco ASA 安全软件 XSS 漏洞通告

报告信息

报告名称	【在野利用 PoC 公开】 CVE-2020-3580: Cisco ASA 安全软件 XSS 漏洞通告		
报告类型	安全漏洞通告	报告编号	B6-2021-063001
报告版本	1	报告日期	2021-06-30
报告作者	360CERT	联系方式	g-cert-report@360.cn
提供方	北京鸿腾智能科技有限公司-360CERT		
接收方			

报告修订记录

报告版本	日期	修订	审核	描述
1	2021-06-30	360CERT	360CERT	撰写报告

目录

1	漏洞简述	4
2	风险等级	5
3	漏洞详情	6
	CVE-2020-3580: ASA、FTD 跨站脚本攻击漏洞	6
4	影响版本	7
5	修复建议	11
	通用修补建议	11
	临时修补建议	11
6	时间线	12
7	参考链接	13
	附录	14
A	产品侧解决方案	14
	360 城市级网络安全监测服务	14
	360 安全分析响应平台	14
	360 本地安全大脑	15
	360 终端安全管理系统	15
B	报告等级说明	17
	严重	17
	高危	17
	中危	18
	低危	19

C	影响面说明.....	21
D	360CERT 内部评分体系	22

360CERT

1 漏洞简述

2021年06月30日，360CERT监测发现 Cisco 于6月28日发布了思科自适应安全软件（ASA）和 Firepower 威胁防御（FTD）软件在野漏洞活跃的风险通告，漏洞编号为CVE-2020-3580，漏洞等级：中危，漏洞评分：6.1。

Cisco ASA 软件、FTD 软件是运行在 Cisco 设备上的通用软件，主要用于服务用户防御和监控网络内部的攻击。

Cisco ASA 软件、FTD 软件因在设备生产时集成，根据用户使用习惯未能得到实时的升级，近期CVE-2020-3580的漏洞利用代码公开，导致攻击者极易利用该漏洞实施攻击。

对此，360CERT 建议广大用户及时将 思科自适应安全软件（ASA）和Firepower威胁防御（FTD）软件 升级到最新版本。与此同时，请做好资产自查以及预防工作，以免遭受黑客攻击。

2 风险等级

360CERT 对该漏洞的评定结果如下

评定方式	等级
威胁等级	中危
影响面	一般
攻击者价值	较高
利用难度	低
360CERT 评分	6.1

3 漏洞详情

3.1 CVE-2020-3580: ASA、FTD 跨站脚本攻击漏洞

CVE: CVE-2020-3580

组件: ASA Software、FTD Software

漏洞类型: 跨站脚本攻击

影响: 管理凭据窃取, 控制网络中的 Cisco 设备

简述: 该漏洞于 2021 年 06 月 24 日公开 PoC, 28 日 Cisco 发布更新通告表示已发现该漏洞的在野利用较为活跃。思科自适应安全软件 (ASA) 和 Firepower 威胁防御 (FTD) 软件存在 XSS 漏洞。导致攻击者可以构造特制的链接诱使用户点击, 即可窃取用户浏览器中的设备管理凭据, 进而接管网络中的 Cisco 设备。

4 影响版本

组件	影响版本	安全版本	受影响的功能
Cisco:ASA Software	9.6	升级到其他安全版本	AnyConnect IKEv2 Remote Access; AnyConnect SSL VPN ; Clientless SSL VPN
Cisco:ASA Software	9.7	升级到其他安全版本	AnyConnect IKEv2 Remote Access; AnyConnect SSL VPN ; Clientless SSL VPN
Cisco:ASA Software	9.8	9.8.4.34	AnyConnect IKEv2 Remote Access; AnyConnect SSL VPN ; Clientless SSL VPN
Cisco:ASA Software	9.9	9.9.2.85	AnyConnect IKEv2 Remote Access; AnyConnect SSL VPN ; Clientless SSL VPN

组件	影响版本	安全版本	受影响的功能
Cisco:ASA Software	9.10	升级到其他安全版本	AnyConnect IKEv2 Remote Access; AnyConnect SSL VPN ; Clientless SSL VPN
Cisco:ASA Software	9.12	9.12.4.13	AnyConnect IKEv2 Remote Access; AnyConnect SSL VPN ; Clientless SSL VPN
Cisco:ASA Software	9.13	9.13.1.21	AnyConnect IKEv2 Remote Access; AnyConnect SSL VPN ; Clientless SSL VPN
Cisco:ASA Software	9.14	9.14.2.8	AnyConnect IKEv2 Remote Access; AnyConnect SSL VPN ; Clientless SSL VPN

组件	影响版本	安全版本	受影响的功能
Cisco:ASA Software	9.15	9.15.1.15	AnyConnect IKEv2 Remote Access; AnyConnect SSL VPN ; Clientless SSL VPN
Cisco:FTD Software	6.2.2	升级到其他安全版本	AnyConnect IKEv2 Remote Access; AnyConnect SSL VPN
Cisco:FTD Software	6.2.3	升级到其他安全版本	AnyConnect IKEv2 Remote Access; AnyConnect SSL VPN
Cisco:FTD Software	6.3.0	升级到其他安全版本	AnyConnect IKEv2 Remote Access; AnyConnect SSL VPN
Cisco:FTD Software	6.4.0	6.4.0.12 (May 2021)	AnyConnect IKEv2 Remote Access; AnyConnect SSL VPN

组件	影响版本	安全版本	受影响的功能
Cisco:FTD Software	6.5.0	升级到其他安全版本	AnyConnect IKEv2 Remote Access; AnyConnect SSL VPN
Cisco:FTD Software	6.6.0	升级到其他安全版本	AnyConnect IKEv2 Remote Access; AnyConnect SSL VPN
Cisco:FTD Software	6.7.0	6.7.0.2	AnyConnect IKEv2 Remote Access; AnyConnect SSL VPN

5 修复建议

5.1 通用修补建议

根据影响版本中的信息，排查并升级到安全版本

5.2 临时修补建议

1. 不随意打开不受信任的链接
2. 在关键的网络设备上关闭浏览器的 javascript 功能

6 时间线

2021-06-28 PoC 在互联网公开

2021-06-28 Cisco 监测到在野利用并发布通告

2021-06-30 360CERT 发布通告

360CERT

7 参考链接

Cisco Security Advisory ASA FTD Update June 28, 2021

360CERT

A 产品侧解决方案

若想了解更多产品信息或有相关业务需求，可移步至 <http://360.net>。

A.1 360 城市级网络安全监测服务

360CERT 的安全分析人员利用 360 安全大脑的 QUAKE 资产测绘平台 (quake.360.cn)，通过资产测绘技术的方式，对该漏洞进行监测。可联系相关产品区域负责人或 (quake#360.cn) 获取对应产品。



A.2 360 安全分析响应平台

360 安全大脑的安全分析响应平台通过网络流量检测、多传感器数据融合关联分析手段，对该类漏洞的利用进行实时检测和阻断，请用户联系相关产品区域负责人或 (shaoyulong#360.cn) 获取对应产品。



A.3 360 本地安全大脑

360 本地安全大脑是将 360 云端安全大脑核心能力本地化部署的一套开放式全场景安全运营平台，实现安全态势、监控、分析、溯源、研判、响应、管理的智能化安全运营赋能。360 本地安全大脑已支持对相关漏洞利用的检测，请及时更新网络神经元（探针）规则和本地安全大脑关联分析规则，做好防护。



A.4 360 终端安全管理系统

360 终端安全管理系统软件是在 360 安全大脑极智赋能下，以大数据、云计算等新技术为支撑，以可靠服务为保障，集防病毒与终端安全管控功能于一体的企业级安全

产品。

360 终端安全管理系统已支持对相关漏洞进行检测和修复，建议用户及时更新漏洞库并安装更新相关补丁。

360终端安全管理系统软件是在360安全大脑极智赋能下，以大数据、云计算等新技术为支撑，以可靠服务为保障，集防病毒与终端安全管控功能于一体的企业级安全产品。

360终端安全管理系统已支持对相关漏洞进行检测和修复，建议用户及时更新漏洞库并安装更新相关补丁。



360安全大脑

赋能

360终端安全管理系统

防病毒	漏洞与补丁管理	终端管控	资产管理
			
✓ 智能引擎 ✓ 病毒查杀 ✓ 本地私云	✓ 漏洞管理 ✓ 补丁管理 ✓ 停服提示	✓ 桌面管理 ✓ 网络控制 ✓ 远程控制	✓ 硬件资产 ✓ 软件资产

B 报告等级说明

360CERT 评分是依托于 CVSS3.1 的评价体系，由 360CERT 进行分数评定的危害评分

严重	
评定标准	<ol style="list-style-type: none"> 1. $9.0 \leq 360CERT \text{ 评分} \leq 10$ 2. Top20 组件 3. PoC/Exp 公开可直接利用 4. 获得系统权限 5. 蠕虫性攻击
危害结果	<ol style="list-style-type: none"> 1. 实施攻击成本低，难度低 2. 直接获得服务器控制权限 3. 直接影响业务服务运行 4. 核心敏感数据泄漏 5. 下载任意文件 6. 易造成资金风险
修复建议	建议在 3 个工作日内对涉及的产品/组件进行修复操作

高危	
评定标准	<ol style="list-style-type: none">1. $7.0 \leq 360CERT$ 评分 < 92. 通用组件3. PoC 公开4. 获得服务/数据库权限
危害结果	<ol style="list-style-type: none">1. 系统/服务/资源垂直越权2. 获得数据库权限3. 可造成资金风险
修复建议	建议在 7 个工作日内对涉及的产品/组件进行修复操作

中危	
评定标准	<ol style="list-style-type: none">1. $4.0 \leq 360\text{CERT 评分} < 7$2. 需要额外的操作步骤方可实现攻击3. 对服务的运行产生影响但不影响功能<ol style="list-style-type: none">(a) 占用存储空间(b) 降低执行效率4. 获得平台用户级权限
危害结果	<ol style="list-style-type: none">1. 需要额外的操作步骤实现危害行为2. 获得平台平行越权3. 任意文件上传4. 难造成资金风险
修复建议	建议在 12 个工作日内对涉及的产品/组件进行修复操作

低危	
评定标准	1. $0 \leq 360\text{CERT 评分} < 4$ 2. 不对服务的运行产生影响
危害结果	暂无
修复建议	建议在 20 个工作日内对涉及的产品/组件进行修复操作

C 影响面说明

影响面说明	
广泛	<ol style="list-style-type: none">1. 影响主体数 > 10w2. 底层依赖库
一般	<ol style="list-style-type: none">1. $5w < \text{影响主体数} < 10w$2. 次级开源库
局限	<ol style="list-style-type: none">1. 影响主体数 < 5w2. 特制版本的

D 360CERT 内部评分体系

360 内部评分体系是 360CERT 安全研究人员经过一系列的数据分析和调查研究，并结合多年的漏洞研究经验最终得出的一套针对漏洞和安全事件的科学评分标准。此套评分体系能够用来评测漏洞和安全事件的严重程度，并帮助确定所需反应的紧急度和重要度。经验证，此评分体系适用于市面上几乎所有的漏洞和安全事件。

360 内部评分体系建立在“CVSS 漏洞评分体系”的基础上，其最终分数是取决于多个指标的公式，最终计算得出的近似的漏洞利用容易程度和漏洞利用的影响。分数范围是 0 到 10，其中最严重的是 10。该分数能较直观地反映漏洞的威胁等级，具体对应规则如下：

分数	威胁等级
9.0 -10.0	严重
7.0 -8.9	高危
4.0 -6.9	中危
0 -3.9	低危