漏洞事件通告

SonicWall SSL-VPN 远程命令执行漏洞通告

360CERT
北京奇虎科技有限公司 | 2021-01-26

报告信息

报告名称	SonicWall SSL-VPN 远程命令执行漏洞通告		
报告类型	漏洞事件通告	**报告编号**	B6-2021-012601
报告版本	1	**报告日期**	2021-01-26
报告作者	360CERT	**联系方式**	cert@360.cn
提供方	北京奇虎科技有限公司		
接收方			

报告修订记录

报告版本	日期	修订	审核	描述
1	2021-01-26	360CERT	360CERT	撰写报告

目录

一、 漏洞档案

漏洞类型	无类型
CVE 编号	暂无
相关厂商	sonicwall
相关组件	sonicwall
威胁等级	高危
影响面	一般
360CERT 评分	8.5
修复方案	通用修补方案/临时修补方案
漏洞发布时间	2021-01-26
报告生成时间	2021-01-26

二、 漏洞简述

2021 年 01 月 26 日，360CERT 监测发现 @darrenmartyn 发布了 SonicWall SSL-VPN 历史版本远程命令执行 的风险通告，事件等级：高危，事件评分：8.5。

SonicWall SSL-VPN 历史版本中存在漏洞，远程攻击者利用 CGI 程序处理逻辑漏洞，构造恶意的 User-Agent，可造成远程任意命令执行，并获得主机控制权限。

@darrenmartyn 已经公开了获取 `nobody`用户权限的攻击代码，可能即将爆发大规模批量攻击

对此，360CERT 建议广大用户好资产自查以及预防工作，以免遭受黑客攻击。

三、 漏洞评级

经过安全技术人员的分析，最终对该漏洞的评定结果如下

评定方式	等级
威胁等级	高危
影响面	一般
360CERT 评分	8.5

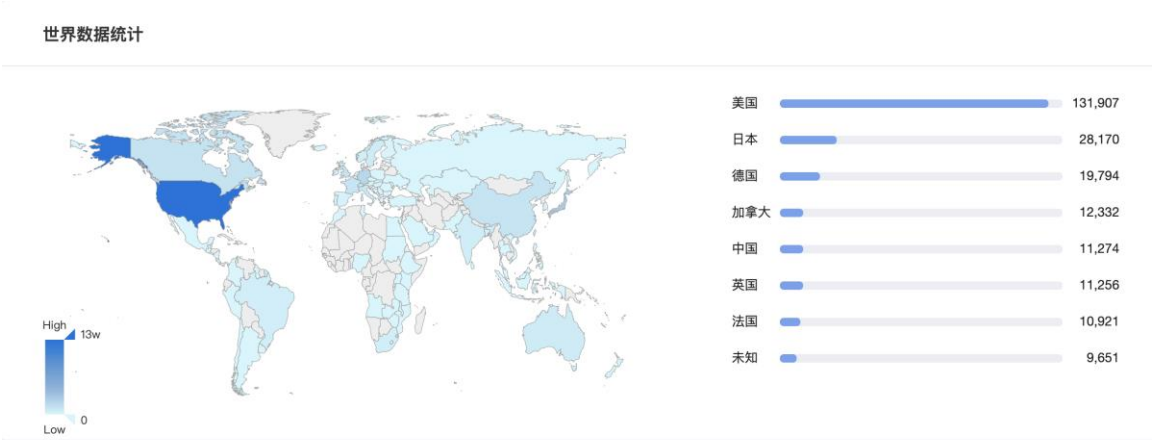
四、 漏洞详情

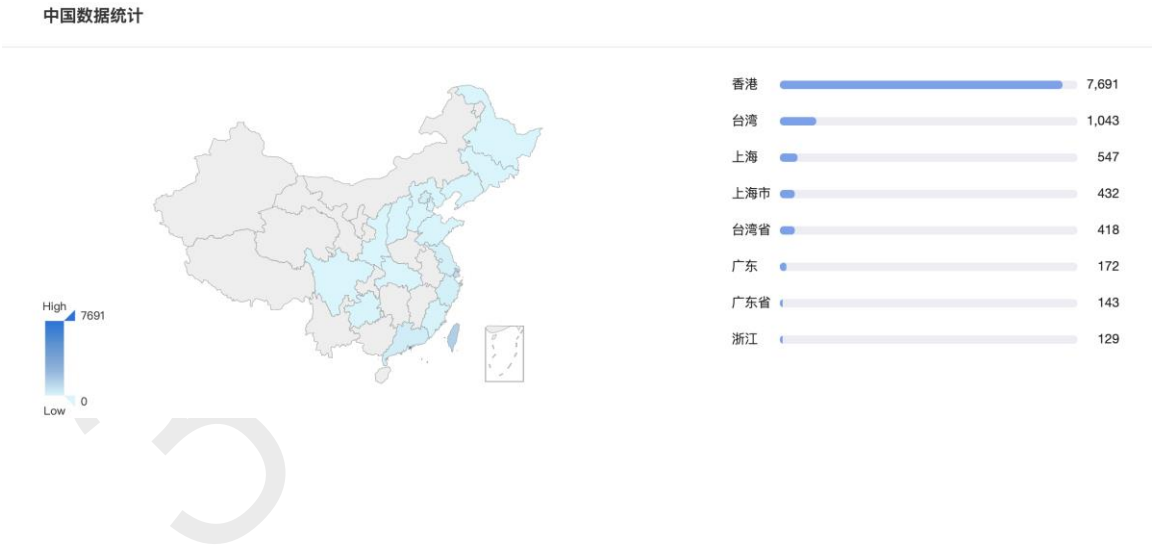
SonicWall SSL-VPN 产品中使用了极为老旧的 Linux 内核和 HTTP CGI 可执行程序，该程序在处理 http 请求时，无法正确的解析 http header。该漏洞导致命令注入，远程攻击者通过注入命令可以轻松的获得 nobody 用户权限的控制权限。

同时由于老旧内核的问题以及其中存在漏洞的可执行程序，攻击者可以轻易的提升权限并完全接管该服务器。

五、 相关空间测绘数据

360 安全大脑-Quake 网络空间测绘系统通过对全网资产测绘，发现 SonicWall SSL-VPN 具体分布如下图所示。





六、 安全建议

(一) 通用修补方案

升级到 Sonic SMA 8.0.0.4

(二) 临时修补方案

针对 http header 进行检测

可能存在的特征字符串如下 () { :; };

使用 nginx 反向代理对 header 进行强制过滤

```
location  /cgi-bin/jarrewrite.sh {
    proxy_pass http://your-ssl-vpn:your-ssl-vpn-port$request_uri;
    proxy_set_header host $http_host;
    proxy_set_header user-agent "sonicwall ssl-vpn rec fix";
}
```

七、 产品侧解决方案

(一) 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。

(二) 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。

八、 参考链接

1. VisualDoor: SonicWall SSL-VPN Exploit

https://darrenmartyn.ie/2021/01/24/visualdoor-sonicwall-ssl-vpn-exploit/

附录 A 报告风险等级说明

360CERT 评分是依托 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	1. 9.0 ≤ 360CERT 评分 ≤ 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	1. 任意攻击者可直接发起攻击 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	1. 7.0 ≤ 360CERT 评分 < 9 2. 通用组件 3. PoC 公开 4. 获得服务/数据库权限
危害结果	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	1. 4.0 ≤ 360CERT 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 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	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 ≤ 360CERT 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

附录 B 影响面说明

影响面说明	
广泛	影响主体数 > 10w 底层依赖库
一般	5w < 影响主体数 < 10w 开源库
局限	影响主体数 < 5w 特制版本的

附录 C 360 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