# 安全漏洞通告

【POC 公开】CVE-2021-20026：SonicWall NSM 认证后命令注入漏洞通告



360CERT
北京奇虎科技有限公司

# 报告信息

| | | | |
|---|---|---|---|
| 报告名称 | 【POC 公开】CVE-2021-20026: SonicWall NSM 认证后命令注入漏洞通告 | | |
| 报告类型 | 安全漏洞通告 | 报告编号 | B6-2021-062501 |
| 报告版本 | 1 | 报告日期 | 2021-06-25 |
| 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 | 2021-06-25 | 360CERT | 360CERT | 撰写报告 |

# 目录

# 1 漏洞简述

2021 年 06 月 25 日，360CERT 监测发现国外安全人员公开了SonicWallNSM认证后命令注入漏洞的 POC。该漏洞最早被 SonicWall 于 2021 年 05 月 27 日预警，漏洞编号为 CVE-2021-20026 ，漏洞等级：高危，漏洞评分：8.8。

SonicWall NSM 主要用于管理 SonicWall 系列的防火墙，准入端点等设备，存在较为广泛的用户群。通过 NSM，管理员可以简单的管理相关安全设备的准入策略，若攻击者获得 NSM 权限，则可以以安全设备流量伪装攻击请求，进行进一步攻击。

该漏洞需要攻击者拥有一个经过认证的用户，同时还需要 NSM 以本地部署的方式部署，攻击面较小，攻击难度大。

对此，360CERT 建议广大用户及时将SonicWallNSM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 | 高危 |
| 影响面 | 广泛 |
| 攻击者价值 | 高 |
| 利用难度 | 中 |
| 360CERT 评分 | 8.8 |

# 3 漏洞详情

## 3.1 CVE-2021-20026: SonicWall NSM 认证后命令注入漏洞

CVE: CVE-2021-20026

组件: SonicWall NSM On-Prem

漏洞类型: 命令注入

影响: 服务器接管

简述: SonicWall NSM On-Prem 产品允许经过身份验证的用户访问一个可执行任意命令的接口，由于其默认存在 python 环境，经过身份验证的攻击者可以构造特制的 POST 请求包访问该端口，通过 python 命令执行任意代码最终造成远程代码执行的效果。

# 4 影响版本

- SonicWall:NSMOn-Prem: <=2.2.0-R10

# 5 修复建议

## 5.1 通用修补建议

将SonicWallNSMOn-Prem产品升级到最新版本（>=2.2.1-R6）。

# 6 时间线

**2021-05-27** SonicWall 官方发布漏洞通告

**2021-06-25** 360CERT 监测到漏洞 POC 公开

**2021-06-25** 360CERT 发布通告

# 7 参考链接

SonicWall 官方漏洞通告

POC 公开情报

# 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 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.2 360 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.3 360 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。


# 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 | 1. 9.0 ≤ 360CERT 评分 ≤ 10<br>2. Top20 组件<br>3. PoC/Exp 公开可直接利用<br>4. 获得系统权限<br>5. 蠕虫性攻击 |
| 危害结果 | 1. 实施攻击成本低，难度低<br>2. 直接获得服务器控制权限<br>3. 直接影响业务服务运行<br>4. 核心敏感数据泄漏<br>5. 下载任意文件<br>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<br>2. 通用组件<br>3. PoC 公开<br>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<br>2. 获得数据库权限<br>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<br>2. 需要额外的操作步骤方可实现攻击<br>3. 对服务的运行产生影响但不影响功能<br>(a) 占用存储空间<br>(b) 降低执行效率<br>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<br>2. 获得平台平行越权<br>3. 任意文件上传<br>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<br>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 | 1. 影响主体数 > 10w<br>2. 底层依赖库 |
| 一般 | 1. 5w < 影响主体数 < 10w<br>2. 次级开源库 |
| 局限 | 1. 影响主体数 < 5w<br>2. 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 |