

安全漏洞通告

CVE-2021-20032: SonicWall Analytics 远程代码执行漏洞通告

报告信息

报告名称	CVE-2021-20032: SonicWall Analytics 远程代码执行漏洞通告		
报告类型	安全漏洞通告	报告编号	B6-2021-081701
报告版本	1	报告日期	2021-08-17
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	2021-08-17	360CERT	360CERT	撰写报告

目录

1	漏洞简述	3
2	风险等级	4
3	漏洞详情	5
	CVE-2021-20032: SonicWall Analytics 远程代码执行漏洞	5
4	影响版本	6
5	修复建议	7
	通用修补建议	7
	临时修补建议	7
6	时间线	8
7	参考链接	9
	附录	10
A	产品侧解决方案	10
	360 安全分析响应平台	10
	360 本地安全大脑	10
	360 终端安全管理系统	11

1 漏洞简述

2021年08月17日, 360CERT 监测发现 SonicWall官方 发布了 SonicWallAnalytics 的风险通告, 漏洞编号为 CVE-2021-20032 , 漏洞等级: 严重, 漏洞评分: 9.8。

SonicWallAnalytics 是一种强大的情报驱动分析服务, 可以解决安全以及网络性能问题, SonicWallAnalytics 的使用场景多, 适配于多种防火墙。

SonicWallAnalytics 默认将 JDWP 接口的调试端口 9000 暴露, 攻击者能够访问该接口, 构造特殊的请求造成远程代码执行。

对此, 360CERT 建议广大用户及时将 SonicWallAnalytics 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	严重
影响面	一般
攻击者价值	高
利用难度	低
360CERT 评分	9.8

3 漏洞详情

3.1 CVE-2021-20032: SonicWall Analytics 远程代码执行漏洞

CVE: CVE-2021-20032

组件: sonicwall analytics on-prem

漏洞类型: 代码执行

影响: 服务器接管

简述:

`SonicWallAnalyticsOn-Prem` 2.5.2518 及之前版本的 `JDWP` 远程调试接口存在漏洞, 该接口默认暴露在 `9000` 端口, 攻击者通过构造特殊的请求, 能够造成远程代码执行, 成功利用该漏洞允许攻击者完全控制受影响的系统。

4 影响版本

组件	影响版本	安全版本
sonicwall analytics on-prem	$\leq 2.5.2518$	$> 2.5.2519$

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

建议 SonicWallAnalytics 的管理员关闭对受影响版本上的 9000/TCP 端口的访问。

6 时间线

2021-08-10 SonicWall 官方发布通告

2021-08-17 360CERT 发布通告

360CERT

7 参考链接

SonicWall 官方通告

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 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。

