安全漏洞通告

CVE-2021-32589：FortiManager & FortiAnalyzer UAF 远程代码执行漏洞通告

360CERT
北京奇虎科技有限公司

报告信息

报告名称	CVE-2021-32589：FortiManager & FortiAnalyzer UAF 远程代码执行漏洞通告		
报告类型	安全漏洞通告	报告编号	B6-2021-072002
报告版本	1	报告日期	2021-07-20
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	2021-07-20	360CERT	360CERT	撰写报告

目录

1 漏洞简述

2021 年 07 月 20 日，360CERT 监测发现 FortiNet官方 发布了 FortiManager&FortiAnalyzerUAF远程代码执行 的风险通告，漏洞编号为 CVE-2021-32589 ，漏洞等级：高危，漏洞评分：7.5。

FortiManager和FortiAnalyzer可以实现集中管理，完成命令控制、网络流量和攻击的报表和分析等功能。UAF（User-After-Free）漏洞存在于FortiManager和FortiAnalyzer 的 fgfmsd守护进程中，攻击者能够以 root 用户的身份执行未经授权的代码。

对此，360CERT 建议广大用户及时将 FortiManager&FortiAnalyzer 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	一般
攻击者价值	高
利用难度	高
360CERT 评分	7.5

3 漏洞详情

3.1 CVE-2021-32589: FortiManager & FortiAnalyzer UAF 远程代码执行漏洞

CVE: CVE-2021-32589

组件: fortimanager & fortianalyzer

漏洞类型: UAF

影响: UAF

简述:

FortiManager和FortiAnalyzer的fgfmsd守护进程中存在UAF（Use-After-Free）漏洞，远程的、未经身份验证的攻击者通过向目标设备的fgfm端口发送专门设计的请求，能够以root用户身的份执行未经授权的代码。

FGFM在FortiAnalyzer上默认是禁用的，只在特定的硬件型号上启用:

1000D,1000E,2000E,3000D,3000E,3000F,3500E,3500F,3700F,3900E。

4 影响版本

组件	影响版本	安全版本
fortimanager & fortianalyzer	<5.6.10	5.6.11
fortimanager & fortianalyzer	<6.0.10	6.0.11
fortimanager & fortianalyzer	<6.2.7	6.2.8
fortimanager & fortianalyzer	<6.4.5	6.4.6
fortimanager & fortianalyzer	<7.0.0	7.0.1
fortimanager	5.4.x	-

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

使用以下命令禁用FortiAnalyzerUnit上的Fortimanager功能：

```
config system global
set fmg-status disable <--- Disabled by default.
end
```

6 时间线

2021-07-19 FortiNet 官方发布通告

2021-07-20 360CERT 发布通告

7 参考链接

FortiNet 官方通告

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。