FortiGate SSH 漏洞分析及防护方案

Content

内容摘要

近日，全球性的网络安全设备供应商 Fortinet（飞塔）所提供的防火墙被曝存在后门，属于高危漏洞。,攻击者可以通过这个后门，直接获取防火墙控制权限，执行攻击行为，比如抓取流量监听、DNS 欺骗、建立隧道进入企业内网等。本文对该漏洞进行了分析及验证方法，并给出相应防护方案。

1. 1 月 12 日凌晨，国外安全研究员爆料 FortiGate 防火墙存在漏洞，并在给出的链接中附上了完整的攻击利用代码；
2. 1 月 12 日 绿盟科技威胁响应中心启动应急响应机制，对爆出的漏洞进行分析，并将分析结果交付相关产品部门；
3. 1 月 13 日，飞塔发布了声明，称该问题在 2014 年就被内部安全审查发现，属于管理协议的 bug。
4. 1 月 13 日，绿盟远程安全评估系统 RSAS 联合广谱扫描平台 Seer，给出受影响设备的全球分布，并发布漏洞检测方法及应对方案。
5. 1 月 15 日，绿盟科技威胁响应中心发布 Fortinet 漏洞分析与防护报告。

绿盟科技威胁响应中心持续关注 FortiGate 防火墙 SSH 后门漏洞事件的进展，如果您需要了解更多信息，请联系：

- 绿盟科技博客
- http://blog.nsfocus.net/
- 绿盟科技威胁响应中心微博
- http://weibo.com/threatresponse
- 绿盟科技微信号
- 搜索公众号 绿盟科技

漏洞基本情况

2016 年 1 月 12 日，绿盟科技威胁响应中心监测到国外社交网站 Twitter 上开始散播 FortiGate 防火墙存在 SSH 后门事件，FortiGate(飞塔防火墙)是 Fortinet（飞塔）公司推出的网络防火墙产品。

消息一经传出，攻击利用代码已经在互联网上传播，扩散速度较快，同时考虑到该设备在中小企业及服务运营商领域应用较为广泛，而且防火墙设备升级需要一定的时间，所以存在较大风险。目前相关情况如下：

什么是 SSH

SSH 是（Secure SHell protocol） 的简写，便于在不安全网络上提供安全的远程登录及其它安全网络服务的协议，保护信息传输的安全性。FortiGate 防火墙用这个协议来保障远程管理过程中的信息传输安全性。

漏洞产生的原因

虽然用了 SSH 来保护信息传输安全，但由于 FortiGate 防火墙 Fortimanager_Access 用户的密码采用了较为简单的算法来生成，并且未对其返回值做特别保护，每次 SSH Fortimanager_Access@xxx.xxx.xx.xx 都可以看到返回一串数字，利用返回的数字结合 exp 中的字符串就能得到验证的密码，攻击者很容易将其破解，从而可以控制防火墙设备，进入企业或组织内部，获取信息或者进行更多攻击行为。

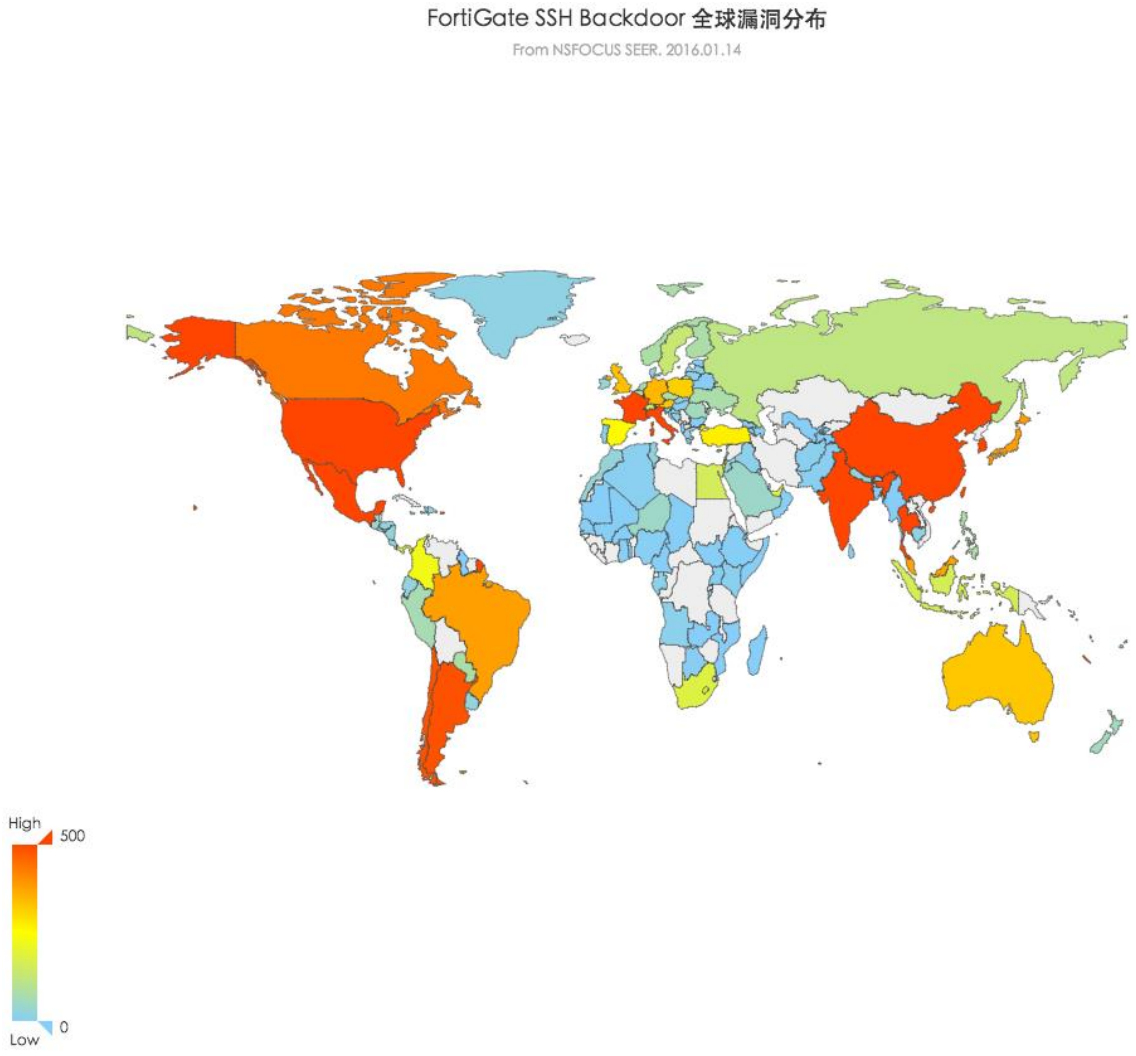
近日，Fortinet（飞塔）公司发布声明称，这是一个 2014 年就被内部安全审查发现的问题，属于管理协议的 bug，而不是主观故意的“后门”，并且暂未接收到用户报告称设备在互联网被黑客攻击。

存在漏洞的设备版本

漏洞影响 FortiNet FortiOS 4.3.0 to 4.3.16 ,FortiNet FortiOS 5.0.0 to 5.0.7 版本 ,而 FortiNet FortiOS 4.3.17 以及更高版本、FortiNet FortiOS 5.0.8 以及更改版本不受影响；

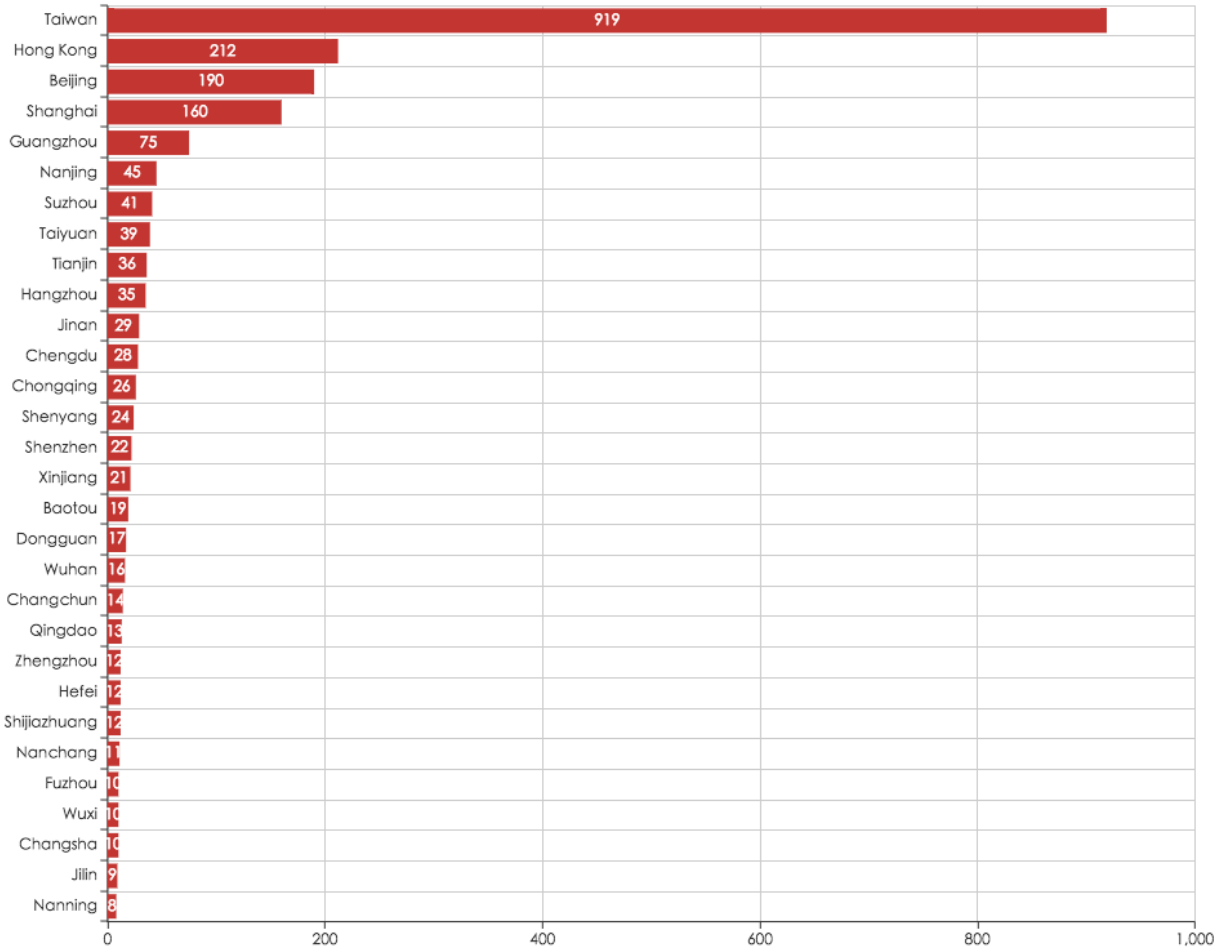
漏洞影响分析

截止到 2016 年 1 月 14 日 ,绿盟科技 Seer 广谱平台检测到互联网上约有 8 万多台 Fortigate 设备 ,其中有 30%的设备存在漏洞，中国范围内存在漏洞的 Fortigate 设备有 2285 台。



这些存在漏洞的设备在国内各城市分布如下，排名前几位的城市包括，台湾（919）、香港（212）、北京（190）、上海（160）、广州（75）。

FortiGate SSH Backdoor 国内城市排名 TOP30

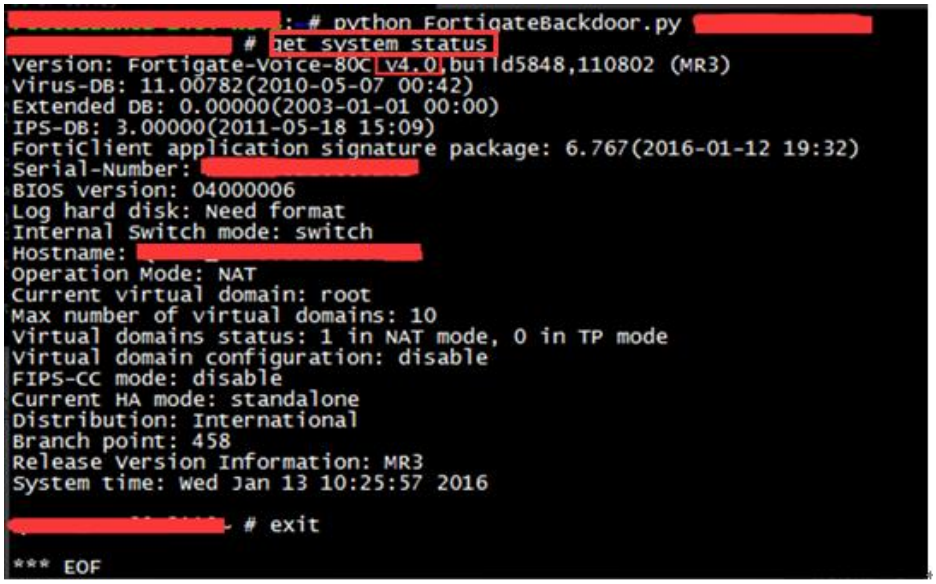


漏洞分析

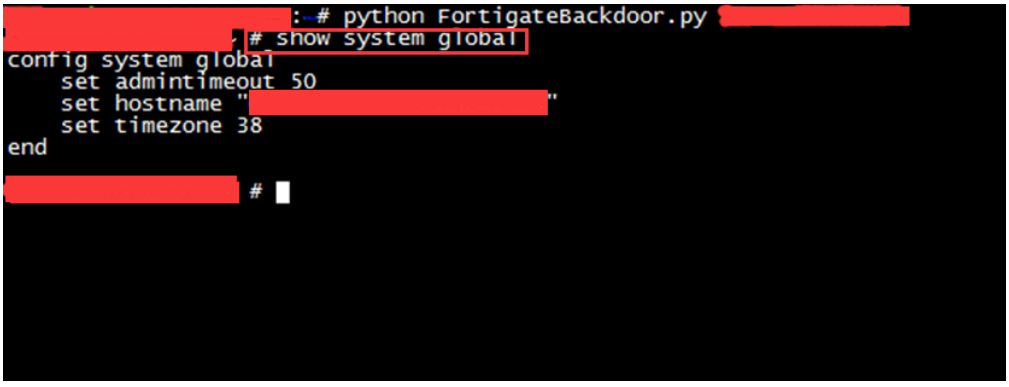
针对网络上流传的 SSH 漏洞，绿盟科技的威胁响应专家对漏洞情况进行了验证，确认该漏洞确认可以导致攻击者控制防火墙的情况发生，同时根据验证过程，给出了漏洞扫描方案，便于各企业及组织对业务环境中的 Fortigate 设备进行安全性评估。

漏洞验证

我们在测试环境中随机选择了一台 FortiGate 设备进行了测试。从如下截图可以看到，利用该 SSH 后门漏洞获得直接控制 Fortigate 设备，执行任意操作。



如果执行“show system global”，则可以看到查看主机名和管理端口命令，显示结果如下：



如果输入“get system status”查看系统状态命令，则可获取 FortiGate 详细的系统信息，包括其设备版本、病毒库、IPS 规则库、FortiClient 应用签名包、序列号、BIOS 版本、主机名、运行模式、虚拟域名状态、系统时间信息等，这些信息的获取将为攻击动作提供极大的便利。

漏洞扫描

绿盟科技建议部署了 FortiGate 防火墙的用户及时自查是否存在该漏洞，以防被恶意攻击者利用。绿盟远程安全评估系统（RSAS）已发布紧急检测插件，请绿盟 RSAS 用户及时到绿盟科技官网的软件升级界面下载相关升级包，对业务资产进行检测。

远程安全评估系统（RSAS）6.0系统插件升级包列表

如果要安装多个升级包，请按照日期先后顺序安装；灰色的升级包无需安装。

名称：rsas-vulsys-V6.0R02F00.0135.dat	版本：V6.0R02F00.0135
MD5：2a591c3a38bb9d7d5f42ca6eb6d920b0	大小：9.29M

描述：
本升级包为系统插件升级包，支持的系统插件版本为V6.0R02F00.0134。升级包为增量升级包，升级后系统版本不变，系统插件版本变更为V6.0R02F00.0135。
新增紧急插件：FortiGate OS (飞塔防火墙) SSH后门漏洞
注意事项：
1. 本升级包升级完成后自动重启引擎生效，升级过程中可能会影响正在使用的功能，请选择在合适的时间进行升级。

发布时间：2016-01-13 15:34:18

此外，绿盟云上的极光自助扫描服务也已实现 FortiGate SSH 后门漏洞的在线检测。绿盟极光自助扫描申请试用页面：

https://cloud.nsfocus.com/#/krosa/views/initcdr/productandservice?pid=0&sid=0

防护方案

固件升级

飞塔公司在其官方网站对此事件进行了说明，虽然没有提供相关补丁，但可以通过版本升级的方式解决该问题，升级的版本信息为：

- FortiOS 分支 4.3:升级到 FortiOS 4.3.17 或更高版本；
- FortiOS 分支 5.0:升级到 FortiOS 5.0.8 或更高版本；

升级办法

升级的方法包括 console 串口命令行、telnet 命令行、web 页面操作等，请所有 FortiGate 相关产品用户，尽快通过其官方渠道下载最新的固件（firmware build）http://support.fortinet.com/

产品防护

请该产品的用户尽早升级固件版本，并采用其入侵防护策略中的《SSH 登录请求认证》策略，加强对 SSH 登录认证请求的排查和防护。

如果条件限制不能及时升级版本，绿盟科技入侵防护产品的安全专家建议：

- 在所有接口禁用通过 SSH 连接进行管理访问，尽量使用 web 界面或串口访问。
- 如果必须使用 SSH 访问，建议利用本地策略进行限制，仅允许最小范围的授权 IP 组访问访问 FortiGate 防火墙。

威胁情报

SECURITY

威胁情报的获取及响应都体现了防御能力的建设程度，威胁情报服务体系至少包含了威胁监测及响应、数据分析及整理、业务情报及交付、风险评估及咨询、安全托管及应用等各个方面，涉及研究、产品、服务、运营及营销的各个环节，绿盟科技通过研究、云端、产品、服务等立体的应急响应体系，向企业和组织及时提供威胁情报，并持续对对匿名者攻击事件进行关注，保障客户业务的顺畅运行。

如果您对我们提供的内容有任何疑问，或者需要了解更多的信息，可以随时通过在微博、微信中搜索绿盟科技联系我们，欢迎您的垂询！

关于绿盟科技

NSFOCUS

北京神州绿盟信息安全科技股份有限公司（简称绿盟科技）成立于 2000 年 4 月，总部位于北京。在国内外设有 30 多个分支机构，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。

基于多年的安全攻防研究，绿盟科技在网络及终端安全、互联网基础安全、合规及安全管理等领域，为客户提供入侵检测/防护、抗拒绝服务攻击、远程安全评估以及 Web 安全防护等产品以及专业安全服务。

北京神州绿盟信息安全科技股份有限公司于 2014 年 1 月 29 日起在深圳证券交易所创业板上市交易，股票简称：绿盟科技，股票代码：300369。