预警编号：YJ-2017035

恒安嘉新

关于 Palo Alto Networks 防火墙操作系统 PAN-OS 存在远程代码执行漏洞

安全预警通告

恒安嘉新（北京）科技股份公司

2017 年 12 月 15 日

1 漏洞描述

近期，互联网爆出 Palo Alto Networks 防火墙操作系统 PAN-OS 远程代码执行漏洞（CVE-2017-15944），允许远程攻击者通过包含管理接口的向量来执行任意代码。漏洞危害程度为高危(High)。

2 影响范围

受影响的版本如下：

<=PAN-OS 6.1.18

<=PAN-OS 7.0.18

<=PAN-OS 7.1.13

<=PAN-OS 8.0.5。

3 漏洞原理

Palo Alto Networks PAN-OS 是美国 Palo Alto Networks 公司为其下一代防火墙设备开发的一套操作系统。2017 年 12 月 12 日，Palo Alto Networks 公司发布了 PAN-OS 安全漏洞公告，修复了 PAN-OS 多个漏洞，通过组合利用这些不相关的漏洞 ,攻击者通过设备的管理接口可以在最高特权用户的上下文中远程执行代码。

4 修复建议

厂商已经修复了该漏洞，请及时更新到 PAN-OS 6.1.19、PAN-OS 7.0.19 PAN-OS 7.1.14、PAN-OS 8.0.6 等版本。详情请关注厂商主页：http://www.paloaltonetworks.com/

如不能及时更新，建议采取如下临时缓解措施：

对管理接口隔离，无论是通过网络分割或是在 PAN-OS 中使用 IP 访问控制列表限制功能都应只允许安全管理员访问，并严格限制其他用户角色访问。