预警编号：YJ-2017011

恒安嘉新

关于摄像机制造商福斯康姆 Foscam 相关产品存在 18 个安全漏洞安全预警通告

恒安嘉新（北京）科技股份公司

2017 年 06 月 12 日

漏洞简介:

近期，福斯康姆 Foscam 相关产品被曝存在 18 个安全漏洞。综合利用漏洞，攻击者可以访问私人视频，并危及连接到同一本地网络的其他设备，永久替换控制照相机的正常固件，并能在不被检测到的情况下重新启动，甚至能够远程控制摄像头，并利用这些 Iot 设备发起大规模 DDOS 攻击。福斯康姆 FOSCAM 产品遍及全球，影响很大。

漏洞原理：

FOSCAM 系列摄像头及其相关产品是由福斯康姆（FOSCAM）集团设计、研发、制造及销售的网络摄像机产品，全球应用十分广泛。

2017 年 6 月 7 日，安全公司 F-Secure 发布报告称，中国摄像机制造商福斯康姆 Foscam 的相关摄像头产品存在 18 个安全漏洞。主要漏洞有不安全的默认凭据和硬编码凭据，攻击者很容易获得未经授权的访问；多个远程命令注入漏洞；全域可写文件和目录允许攻击者修改代码并获得 root 权限；隐藏的 telnet 功能允许攻击者使用 telnet 在设备和周围网络中的发现其他漏洞；防火墙配置不当漏洞等。综合利用漏洞，攻击者可以访问私人视频，并危及连接到同一本地网络的其他设备，还可以永久替换控制照相机的正常固件，并能在不被检测到的情况下重新启动。甚至能够远程控制摄像头，并利用这些 Iot 设备发起大规模 DDOS 攻击。

影响范围：

一.Model Name	System	Firmware Version	Application Firmware Version
Opticam	i5	1.5.2.11	2.21.1.128
Foscam	C2	1.11.1.8	2.72.1.32

出现漏洞的产品还涉及其它 14 个品牌:

Chacon、Thomson、7links、Opticam、Netis、Turbox、Novodio、Ambientcam、Nexxt、Technaxx、Qcam、Ivue、Ebode、Sab

修复建议:

1.厂商目前还未修复这些漏洞，请及时关注厂商主页进行更新：

http://www.foscam.com.cn/

2.临时防护建议：

强烈建议用户在没有访问其他连接设备的专用本地网络中运行这些设备，并且确保无法从外部网络访问，尽量确保更改所有默认密码并定期检查安全更新。

参考链接：

https://business.f-secure.com/foscam_cameras_and_compromise

http://images.news.f-secure.com/Web/FSecure/%7B43df9e0d-20a8-404a-86d0-70dcca00b6e5%7D_vulnerabilities-in-foscam-IP-cameras_report.pdf?_ga=2.103952768.1877007297.1496980664-1350286355.1496980664 （详细报告链接）