国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2017 年 06 月 05 日-2017 年 06 月 11 日 **2017 年第 24 期**

本周漏洞态势研判情况

本周信息安全漏洞威胁整体评价级别为**中**。

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 326 个，其中高危漏洞 147 个、中危漏洞 163 个、低危漏洞 16 个。漏洞平均分值为 6.22。本周收录的漏洞中，涉及 0day 漏洞 144 个（占 44%），其中互联网上出现“WordPress console contact form 插件文件上传漏洞、PlaySMS 远程代码执行漏洞（CNVD-2017-08174）”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 1067 个，与上周（766）环比增长 39%。

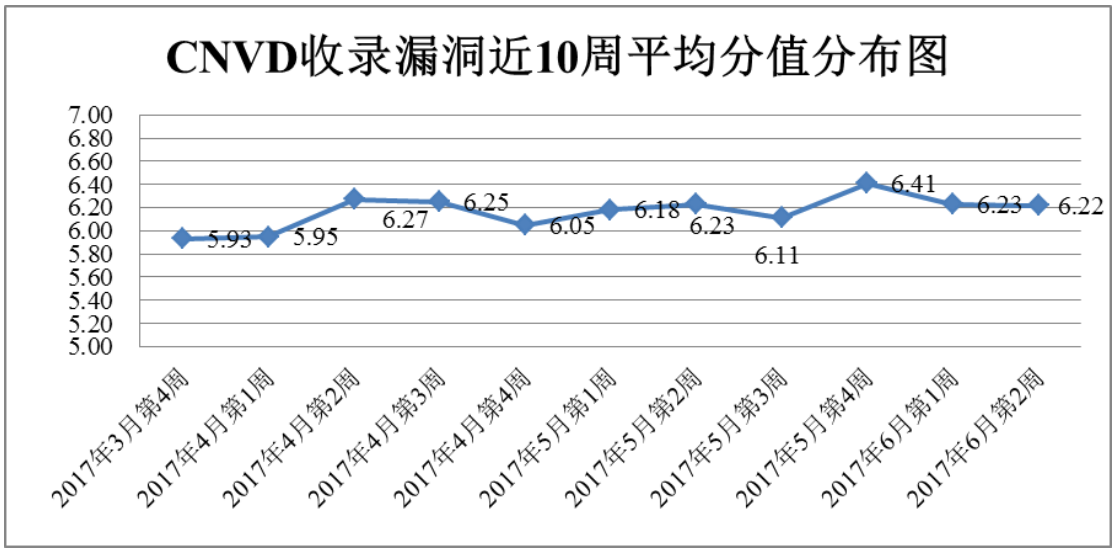

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周，共 19 家成员单位、企业用户及个人用户报送了本周收录的全部 326 个漏洞。报送情况如表 1 所示。其中，启明星辰、华为技术有限公司、天融信、安天实验室、恒安嘉新等单位报送数量较多。360 网神、漏洞盒子、河北网信智安信息技术有限公司、广

州软云计算机科技有限公司、中新网络信息安全股份有限公司、广州神月信息安全技术有限公司、福建六壬网安股份有限公司、江西安服信息产业有限公司、清远职业技术学院、江苏同袍信息科技有限公司、安徽新华博信息技术股份有限公司、安元实验室、北京安码科技有限公司、上海犇众信息技术有限公司及其他个人白帽子向 CNVD 提交了 1067 个以事件型漏洞为主的原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
360 网神	238	238
漏洞盒子	205	205
恒安嘉新	162	1
安天实验室	154	0
天融信	102	2
华为技术有限公司	83	0
启明星辰	62	15
H3C	52	0
杭州安恒信息技术有限公司	37	0
中国电信集团系统集成有限责任公司	35	0
绿盟科技	35	0
厦门服云信息科技有限公司	30	2
阿里云计算有限公司	24	0
知道创宇	7	6
北京数字观星科技有限公司	5	0
卫士通信息产业股份有限公司	4	0
南京铱迅信息技术股份有限公司	3	3
北京无声信息技术有限公司	2	0
西安四叶草信息技术	1	1

有限公司		
河北网信智安信息技术有限公司	27	27
广州软云计算机科技有限公司	26	26
中新网络信息安全股份有限公司	13	13
广州神月信息安全技术有限公司	10	10
福建六壬网安股份有限公司	7	7
江西安服信息产业有限公司	6	6
清远职业技术学院	4	4
江苏同袍信息科技有限公司	2	2
安徽新华博信息技术股份有限公司	1	1
安元实验室	1	1
北京安码科技有限公司	1	1
上海犇众信息技术有限公司	1	1
CNCERT 天津分中心	6	6
CNCERT 宁夏分中心	5	5
CNCERT 北京分中心	3	3
CNCERT 吉林分中心	3	3
CNCERT 广东分中心	2	2
CNCERT 陕西分中心	1	1
CNCERT 上海分中心	1	1
个人报送者	474	474
报送总计	1835	1067
录入总计	326（去重）	1067

表 1 漏洞报送情况统计表

本周漏洞按类型和厂商统计

本周，CNVD 收录了 326 个漏洞。其中应用程序漏洞 150 个，web 应用漏洞 104 个，操作系统漏洞 33 个，网络设备漏洞 30 个，安全产品漏洞 8 个，数据库漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	150
web 应用漏洞	104
操作系统漏洞	33
网络设备漏洞	30
安全产品漏洞	8
数据库漏洞	1

表 2 漏洞按影响类型统计表

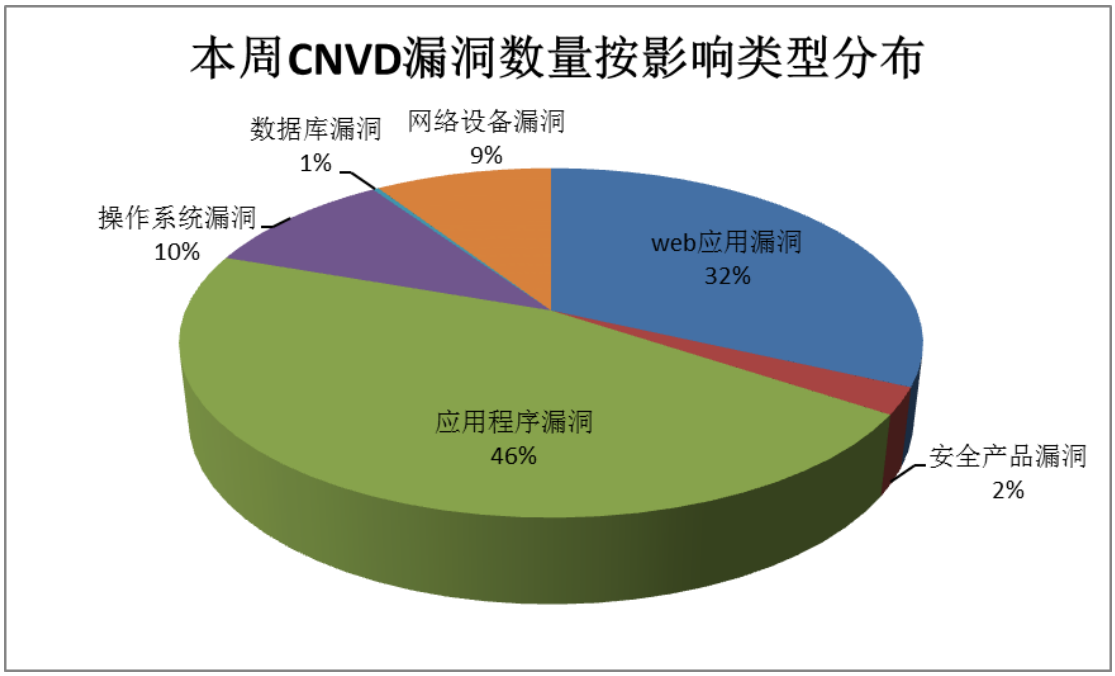

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 AutoTrace、Google、Foscam 等多家厂商的产品，部分漏洞数量按厂商统计如表 3 所示。

序号	厂商（产品）	漏洞数量	所占比例
1	AutoTrace	49	15%
2	Google	24	7%
3	Foscam	18	6%
4	WordPress	18	6%
5	Fastspot	12	4%

6	IBM	10	3%
7	Huawei	10	3%
8	Trend Micro	10	3%
9	Microsoft	7	2%
10	其他	168	51%

表 3 漏洞产品涉及厂商分布统计表

本周行业漏洞收录情况

本周，CNVD 收录了 4 个电信行业漏洞，25 个移动互联网行业漏洞，6 个工控系统行业漏洞（如下图所示）。其中，“多款 Rockwell Automation 产品存在未明漏洞、多款 Rockwell Automation 产品存在未明漏洞（CNVD-2017-08711）、

Google Android HTC bootloader 权限提升漏洞、Google Android Goodix touchscreen driver 权限提升漏洞、Google Android Motorola bootloader 权限提升漏洞”等的综合评级为“高危”。相关厂商已经发布了上述漏洞的修补程序，请参照 CNVD 相关行业漏洞库链接。

电信行业漏洞链接：http://telecom.cnvd.org.cn/

移动互联网行业漏洞链接：http://mi.cnvd.org.cn/

工控系统行业漏洞链接：http://ics.cnvd.org.cn/

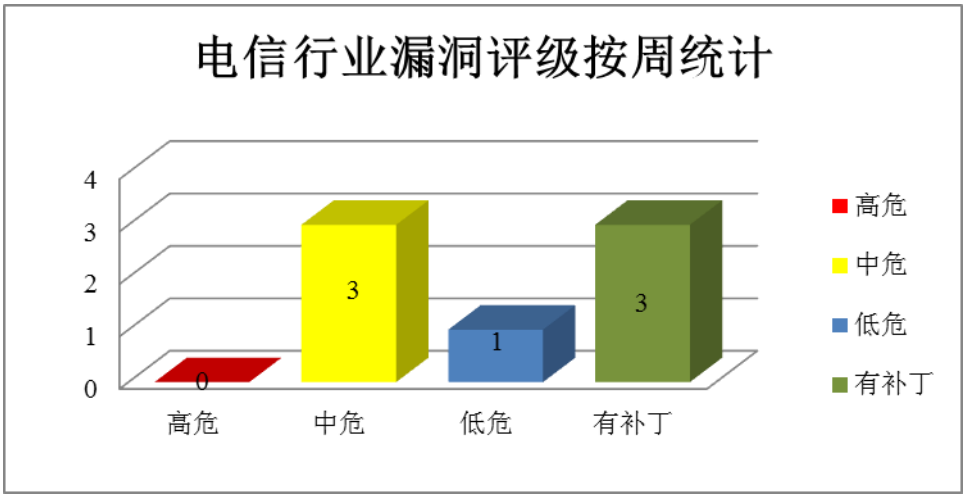

图 3 电信行业漏洞统计

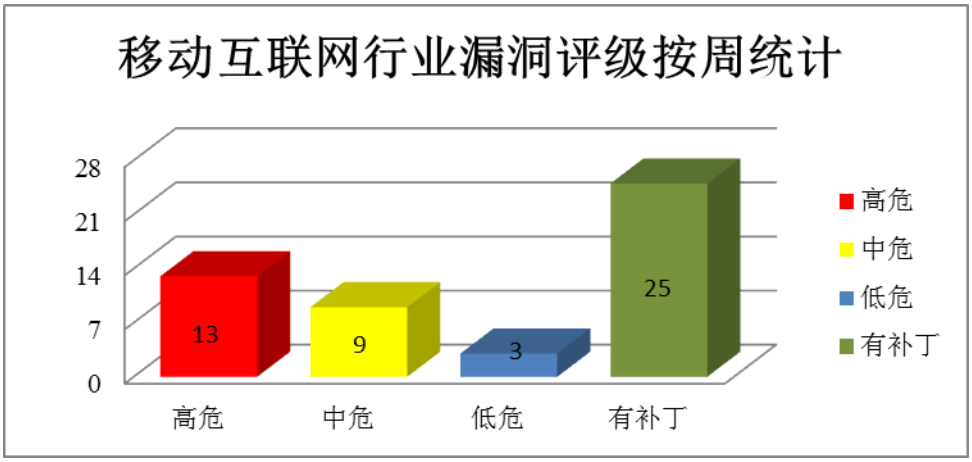

图 4 移动互联网行业漏洞统计

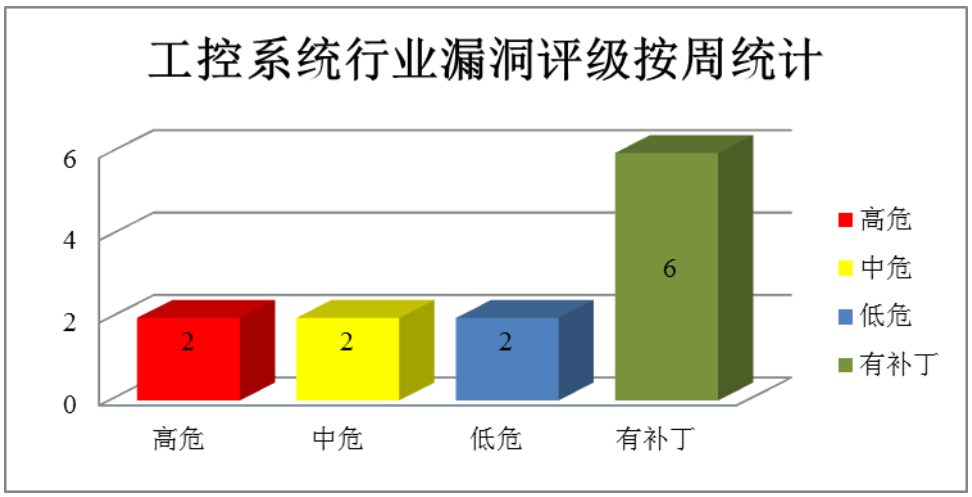

图 5 工控系统行业漏洞统计

本周重要漏洞安全告警

本周，CNVD 整理和发布以下重要安全漏洞信息。

1、Foscam 相关产品安全漏洞

Foscam camera 是一款网络摄像机，可以推送消息到手机，还可直接通过 WIFI 实现视频百度云存储。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞泄露敏感信息和执行任意命令等。

CNVD 收录的相关漏洞包括：Foscam camera ONVIF 重启漏洞、Foscam camera Telnet 功能命令注入漏洞、Foscam camera FTP 服务器帐号空密码漏洞、Foscam camera FTP 服务器帐号硬编码密码漏洞、Foscam camera ONVIF GetStreamUri 管理员凭证泄露漏洞、Foscam camera Web 用户界面隐藏硬编码凭证漏洞、Foscam camera 目录权限分配不当漏洞、Foscam camera 配置备份文件受硬编码保护漏洞。上述漏洞的综合评级为“高危”。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2017-08903

http://www.cnvd.org.cn/flaw/show/CNVD-2017-08905

http://www.cnvd.org.cn/flaw/show/CNVD-2017-08907
http://www.cnvd.org.cn/flaw/show/CNVD-2017-08909
http://www.cnvd.org.cn/flaw/show/CNVD-2017-08898
http://www.cnvd.org.cn/flaw/show/CNVD-2017-08910
http://www.cnvd.org.cn/flaw/show/CNVD-2017-08908
http://www.cnvd.org.cn/flaw/show/CNVD-2017-08897

2、Google 产品安全漏洞

Google Android 是一款基于 Linux 的应用于智能手机设备的操作系统。本周，该产品被披露存在权限提升漏洞，攻击者可利用漏洞提升权限。

CNVD 收录的相关漏洞包括：Google Android Goodix touchscreen driver 权限提升漏洞、Google Android HTC bootloader 权限提升漏洞、Google Android kernel trace subsystem 权限提升漏洞、Google Android Motorola bootloader 权限提升漏洞、Google Android Qualcomm crypto driver 权限提升漏洞、Google Android Qualcomm LED driver 权限提升漏洞、Google Android Qualcomm pin controller driver 权限提升漏洞、Google Android Qualcomm power driver 权限提升漏洞。上述漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2017-08231
http://www.cnvd.org.cn/flaw/show/CNVD-2017-08232
http://www.cnvd.org.cn/flaw/show/CNVD-2017-08234
http://www.cnvd.org.cn/flaw/show/CNVD-2017-08237
http://www.cnvd.org.cn/flaw/show/CNVD-2017-08225
http://www.cnvd.org.cn/flaw/show/CNVD-2017-08224
http://www.cnvd.org.cn/flaw/show/CNVD-2017-08226
http://www.cnvd.org.cn/flaw/show/CNVD-2017-08295

3、Huawei 存在多个漏洞

Huawei HedEx Lite 是中国华为（Huawei）公司的一款文档管理软件。Huawei iManager NetEco 是一款机房动环监控系统。Huawei P7、P8 青春版和 P9 Plus 都是智能手机设备。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限或执行任意命令或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Huawei HedEx Lite DLL 劫持漏洞、Huawei HedEx Lite 跨站脚本漏洞、Huawei HedEx Lite 跨站请求伪造漏洞、Huawei HedEx Lite 任意文件下载漏洞、Huawei Manager NetEco 命令注入漏洞、Huawei P7 GPU 驱动程序权限提升漏洞、Huawei P7 和 P8 青春版拒绝服务漏洞、Huawei P9 Plus 内存错误引用漏洞。上述漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CN

VD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2017-08774

http://www.cnvd.org.cn/flaw/show/CNVD-2017-08776

http://www.cnvd.org.cn/flaw/show/CNVD-2017-08775

http://www.cnvd.org.cn/flaw/show/CNVD-2017-08773

http://www.cnvd.org.cn/flaw/show/CNVD-2017-08781

http://www.cnvd.org.cn/flaw/show/CNVD-2017-08782

http://www.cnvd.org.cn/flaw/show/CNVD-2017-08780

http://www.cnvd.org.cn/flaw/show/CNVD-2017-08778

4、WordPress 产品安全漏洞

WordPress 是 WordPress 软件基金会的一套使用 PHP 语言开发的博客平台本周，该产品被披露存在权限提升、文件上传和 SQL 注入漏洞，攻击者可利用漏洞提升权限、上传任意文件和泄露数据库敏感信息等。

CNVD 收录的相关漏洞包括：WordPress Bulk Delete 插件权限提升漏洞、WordPress console contact form 插件文件上传漏洞、WordPress Huge-IT Video Gallery 插件 SQL 注入漏洞、WordPress Ocim MP3 插件 SQL 注入漏洞、Wordpress Themes Purevision 任意文件上传漏洞、Wordpress Themes rehber 文件上传漏洞、Wordpress 插件 dopts 文件上传漏洞、WordPress 插件 Huge-IT Video Gallery SQL 注入漏洞。上述漏洞的综合评级为“高危”。目前，厂商已经发布了“WordPress Huge-IT Video Gallery 插件 SQL 注入漏洞、WordPress 插件 Huge-IT Video Gallery SQL 注入漏洞、WordPress Bulk Delete 插件权限提升漏洞”的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2017-08915

http://www.cnvd.org.cn/flaw/show/CNVD-2017-08935

http://www.cnvd.org.cn/flaw/show/CNVD-2017-08917

http://www.cnvd.org.cn/flaw/show/CNVD-2017-08916

http://www.cnvd.org.cn/flaw/show/CNVD-2017-08921

http://www.cnvd.org.cn/flaw/show/CNVD-2017-08933

http://www.cnvd.org.cn/flaw/show/CNVD-2017-08931

http://www.cnvd.org.cn/flaw/show/CNVD-2017-08514

5、Fastspot BigTree CMS 任意代码执行漏洞

Fastspot BigTree CMS 是美国 Fastspot 公司的一套基于 PHP 和 MySQL 的开源内容管理系统。本周，Fastspot 被披露存在任意代码执行漏洞，攻击者可利用漏洞执行任意代码。目前，互联网上已经出现了针对该漏洞的攻击代码，厂商尚未发布漏洞修补程序。CNVD 提醒广大用户随时关注厂商主页，以获取最新版本。

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2017-08703

更多高危漏洞如表 4 所示，详细信息可根据 CNVD 编号，在 CNVD 官网进行查询。

参考链接:http://www.cnvd.org.cn/flaw/list.htm

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2017-08187	EMC Isilon OneFS 远程权限提升漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页：https://www.emc.com/
CNVD-2017-08183	Mimosa Client Radios 信息泄露漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页：http://www.mimosa.co/
CNVD-2017-08189	Gongwalker API Manager 跨站请求伪造漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://github.com/gongwalker/ApiManager
CNVD-2017-08190	Pivotal RabbitMQ 产品跨站脚本漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：http://www.pivota.com
CNVD-2017-08217	Open Source Solutions ViMbAdmin 跨站请求伪造漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.vimbadmin.net/
CNVD-2017-08297	GNU C Library 'xdr_bytes'和'xdr_string'函数拒绝服务漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞:https://www.gnu.org/
CNVD-2017-08299	Cerberus FTP Server 远程缓冲区溢出漏洞（CNVD-2017-08299）	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.cerberusftp.com/
CNVD-2017-08710	多款 Rockwell Automation 产品存在未明漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页：http://rockwellautomation.com/
CNVD-2017-08793	rpcbind、LIBTIRPC 和 NTIRPC 拒绝服务漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞:https://github.com/guidovranken/rpcbomb/
CNVD-2017-08796	iRODS 远程命令执行漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞:https://github.com/irods/irods/issues/3452

表 4 部分重要高危漏洞列表

小结：本周，Foscam 被披露存在多个漏洞，攻击者可利用漏洞泄露敏感信息和执

行任意命令等。此外，Google、Huawei、Wordpress 等多款产品被披露存在多个漏洞，攻击者利用漏洞可执行任意代码、上传任意文件、提升权限或发起拒绝服务攻击等。另外，Fastspot 被披露存在任意代码执行漏洞，攻击者可利用漏洞执行任意代码。建议相关用户随时关注上述厂商主页，及时获取修复补丁或解决方案。

本周漏洞要闻速递

1. 国内 Foscam 制造的 IP 摄像头被曝出大量漏洞

近期，研究人员在国内 Foscam 制造的 IP 摄像头中发现了大量安全漏洞。据了解，这些漏洞其实早在几个月前就已经上报给厂商了，但直到目前为止我们仍然没有拿到可用的更新补丁。由于很多品牌的产品都使用了 Foscam 摄像头，因此我们建议广大用户确定自己 IP 摄像头的制造商，如果有必要的话还需要用户自己动手采取缓解措施。

参考链接：http://www.freebuf.com/vuls/136794.html

2. FreeRADIUS 服务器中存在 TLS 认证绕过漏洞

近期，来自卢森堡 RESTENA 的安全研究专家 Stefan Winter 在当前全球最流行的 radius 服务器中发现了一个 TLS 认证绕过漏洞。这个漏洞（CVE-2017-9148）存在于 TTLS 和 PEAP 实现之中，当系统在处理重连的 TLS 链接时便会触发这个漏洞，此时攻击者将能够绕过系统的内部验证机制。正在使用 FreeRADIUS 的系统管理员们需要将版本更新至 3.0.14 方可解决这个问题，目前临时的缓解方案为禁用 TLS 会话缓存。

参考链接：http://www.freebuf.com/vuls/136071.html

关于 CNVD

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库，致力于建立国家统一的信息安全漏洞收集、发布、验证、分析等应急处理体系。

关于 CNCERT

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称是 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，为非政府非盈利的网络安全技术中心，是我国网络安全应急体系的核心协调机构。

作为国家级应急中心，CNCERT 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82990999