

信息安全漏洞周报

2018 年 3 月 19 日-2018 年 3 月 25 日

2018 年第 12 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 487 个，其中高危漏洞 173 个、中危漏洞 282 个、低危漏洞 32 个。漏洞平均分为 6.04。本周收录的漏洞中，涉及 0day 漏洞 105 个（占 22%），其中互联网上出现“Joomla! Ek Rishta SQL 注入漏洞、Seagate BlackArmor NAS 远程代码执行漏洞”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 438 个，与上周（622 个）环比下降 30%。

CNVD收录漏洞近10周平均分分布图

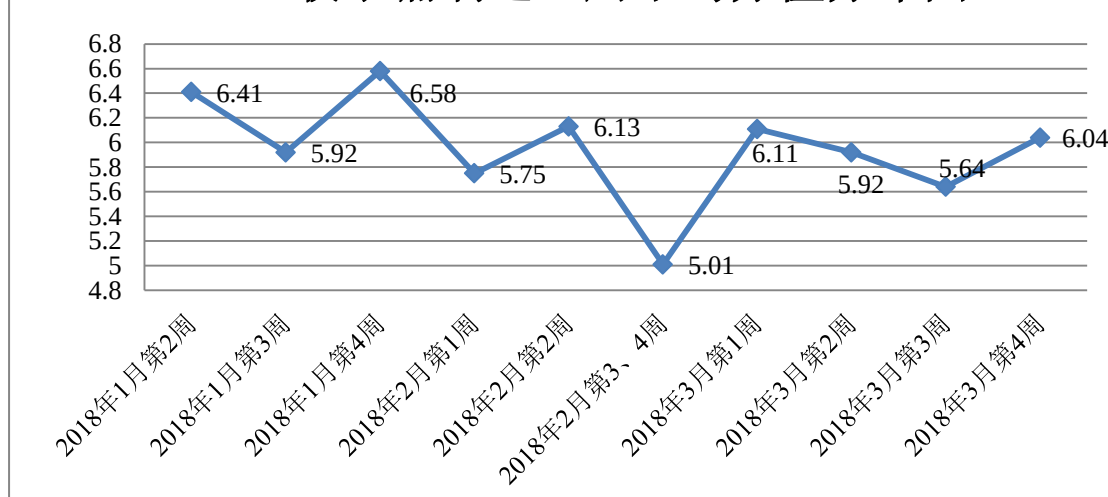


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京天融信网络安全技术有限公司、北京启明星辰信息技术有限公司、哈尔滨安天科技股份有限公司、华为技术有限公司、中国电信集团系统集成有限责任公司等单位报送公开收集的漏洞数量较多。四川虹微技术有限

公司（子午攻防实验室）、中新网络信息安全股份有限公司、福建榕基软件股份有限公司、上海观安信息技术股份有限公司、南京联成科技发展股份有限公司、南瑞集团公司（国网电力科学研究院）、安徽三实信息技术服务有限公司、杭州安信检测技术有限公司、天罡(横琴)网络科技有限公司、上海市信息安全测评认证中心及其他个人白帽子向 CNVD 提交了 438 个以事件型漏洞为主的原创漏洞，其中包括 360 网神（补天平台）和漏洞盒子向 CNVD 共享的白帽子报送的 227 条原创漏洞信息。

表 1 漏洞报送情况统计表

报送单位或个人	漏洞报送数量	原创漏洞数量
北京天融信网络安全技术有限公司	364	1
北京启明星辰信息安全技术有限公司	213	0
哈尔滨安天科技股份有限公司	199	0
华为技术有限公司	194	0
360 网神（补天平台）	131	131
漏洞盒子	96	96
中国电信集团系统集成有限责任公司	90	1
北京数字观星科技有限公司	91	0
北京神州绿盟科技有限公司	82	0
恒安嘉新(北京)科技股份有限公司	80	0
新华三技术有限公司	80	0
卫士通信息产业股份有限公司	12	0
北京无声信息技术有限公司	7	0
深圳市深信服电子科技有限公司	1	1
四川虹微技术有限公司（子午攻防实验室）	34	34
中新网络信息安全股份有限公司	10	10
福建榕基软件股份有限公司	5	5

上海观安信息技术股份有限公司	3	3
南京联成科技发展股份有限公司	3	3
南瑞集团公司（国网电力科学研究院）	2	2
安徽三实信息技术服务有限公司	2	2
杭州安信检测技术有限公司	2	2
天罡(横琴)网络科技有限公司	1	1
上海市信息安全测评认证中心	1	1
CNCERT 山西分中心	15	15
CNCERT 天津分中心	5	5
CNCERT 新疆分中心	1	1
CNCERT 河北分中心	1	1
CNCERT 广东分中心	1	1
个人	122	122
报送总计	1848	438

本周漏洞按类型和厂商统计

本周，CNVD 收录了 487 个漏洞。其中应用程序漏洞 248 个，WEB 应用漏洞 115 个，操作系统漏洞 71 个，网络设备漏洞 44 个，安全产品漏洞 6 个，数据库漏洞 3 个。

表 2 漏洞按影响类型统计表

漏洞影响对象类型	漏洞数量
应用程序漏洞	248
WEB 应用漏洞	115
操作系统漏洞	71
网络设备漏洞	44
安全产品漏洞	6
数据库漏洞	3

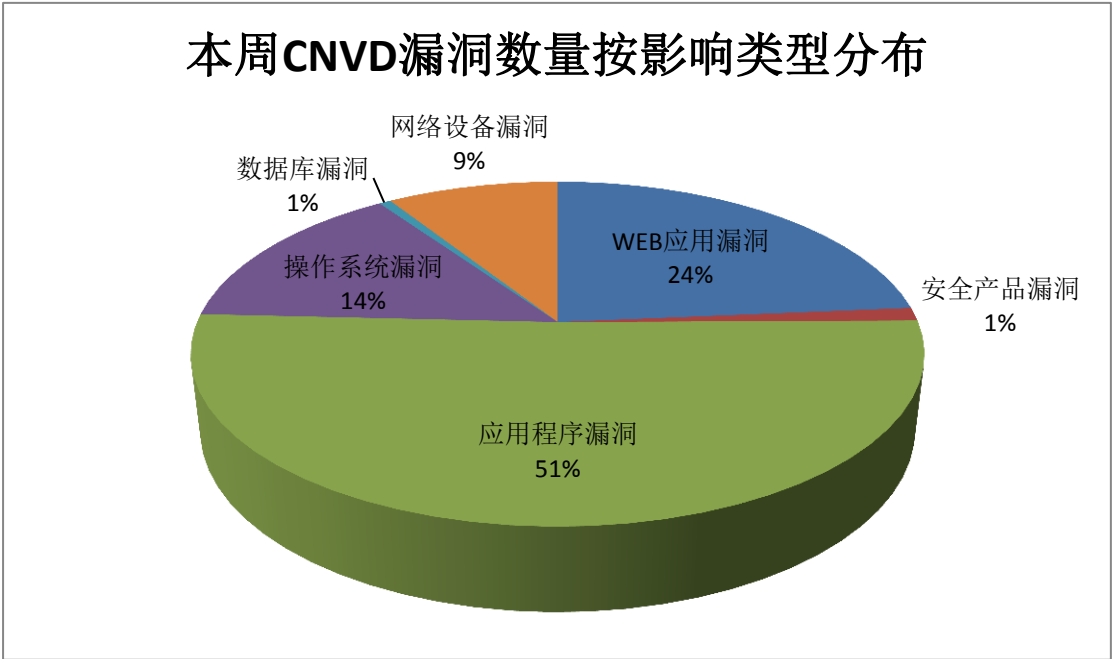


图 2 本周漏洞按影响类型分布

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

表 3 漏洞产品涉及厂商分布统计表

序号	厂商（产品）	漏洞数量	所占比例
1	Microsoft	35	7%
2	Google	34	7%
3	IBM	10	2%
4	Foxit	8	2%
5	Joomla!	8	2%
6	Atlassian	7	2%
7	eQ-3 AG	6	1%
8	Geutebruck	6	1%
9	Linux	6	1%
10	其他	367	75%

本周行业漏洞收录情况

本周，CNVD 收录了 10 个电信行业漏洞，45 个移动互联网行业漏洞，12 个工控行业漏洞（如下图所示）。其中，“MikroTik RouterOS 缓冲区溢出漏洞、ZyXEL P-870H-51 DSL Router CGI 拒绝服务漏洞、Geutebruck IP Cameras SQL 注入漏洞、HP Load

Runner 和 Performance Center 远程代码执行漏洞、Google Android Qualcomm Wma 权限提升漏洞”等漏洞的综合评级为“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/>

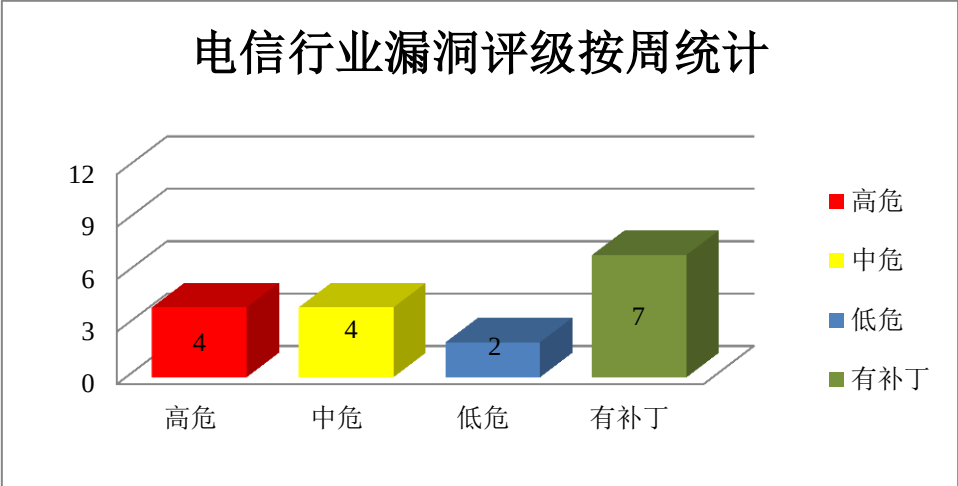


图 3 电信行业漏洞统计

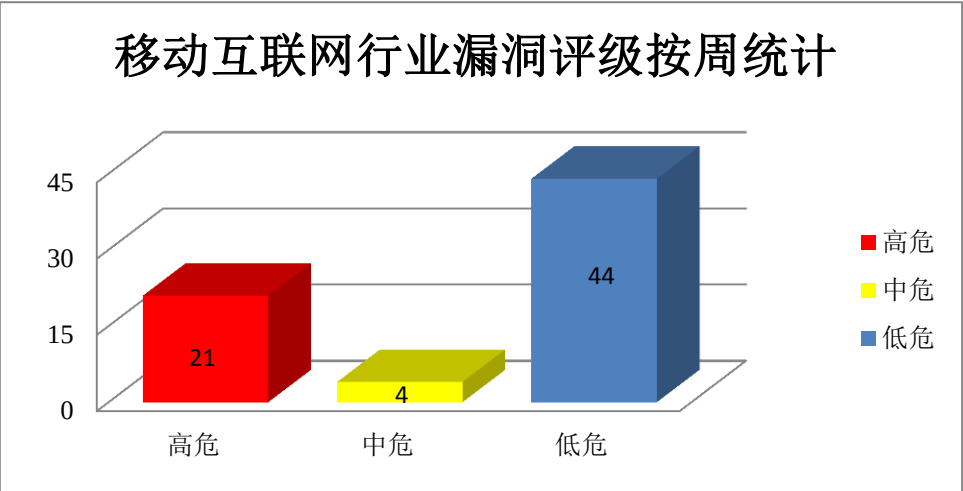


图 4 移动互联网行业漏洞统计

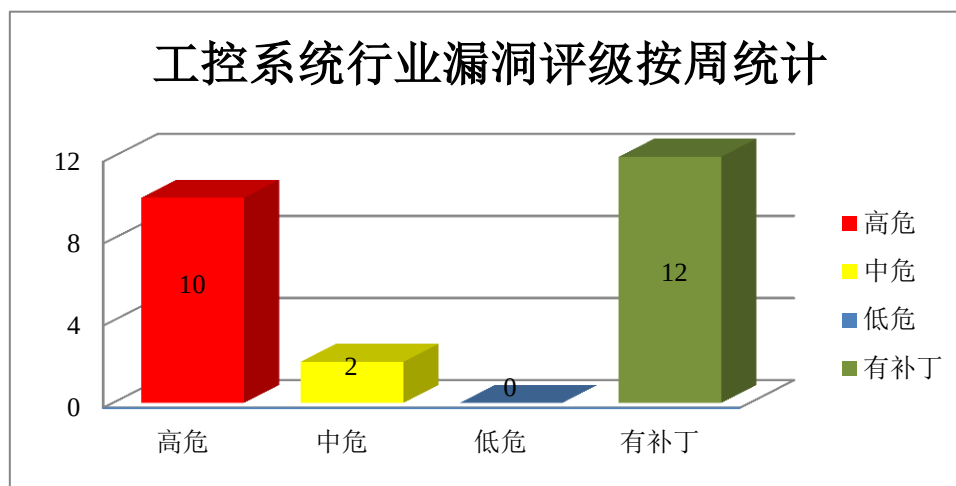


图 5 工控行业漏洞统计

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、Google 产品安全漏洞

Android 是一种基于 Linux 的自由及开放源代码的操作系统，Qualcomm Wma 是其中的一个美国高通公司的 Wma（数字音频压缩格式）组件。Qualcomm WLAN 是无线局域网组件。本周，该产品被披露存在权限提升漏洞，攻击者可利用漏提升权限。

CNVD 收录的相关漏洞包括：Google Android Qualcomm Wma 权限提升漏洞（CNVD-2018-06011、CNVD-2018-06009、CNVD-2018-06007、CNVD-2018-06006、CNVD-2018-06005）、Google Android Qualcomm WLAN 权限提升漏洞（CNVD-2018-05998、CNVD-2018-05996、CNVD-2018-05992）。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-2018-06011>
<http://www.cnvd.org.cn/flaw/show/CNVD-2018-06009>
<http://www.cnvd.org.cn/flaw/show/CNVD-2018-06007>
<http://www.cnvd.org.cn/flaw/show/CNVD-2018-06006>
<http://www.cnvd.org.cn/flaw/show/CNVD-2018-06005>
<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05998>
<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05996>
<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05992>

2、Microsoft 产品安全漏洞

Microsoft Windows 10 等都是美国微软公司发布的一系列操作系统。Windows Shell 是一个 Windows 系统下与用户交互的界面。StructuredQuery 是一个结构化查询组件。

Microsoft Office 是一款办公软件套件产品。Edge 是其中的一个系统附带的浏览器。Microsoft Access 是一套关系数据库管理系统。本周，上述产品被披露存在代码执行漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Windows Shell 远程代码执行漏洞（CNVD-2018-05838）、Microsoft StructuredQuery 远程代码执行漏洞、Microsoft Office 任意代码执行漏洞（CNVD-2018-05885）、Microsoft Edge 和 ChakraCore 远程代码执行漏洞、Microsoft ChakraCore 远程代码执行漏洞（CNVD-2018-05887CNVD-2018-05734）、Microsoft ChakraCore 和 Edge 远程代码执行漏洞、Microsoft Access 任意代码执行漏洞。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-2018-05838>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05742>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05885>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05888>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05887>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05734>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05889>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05840>

3、Joomla!产品安全漏洞

Joomla!是一套开源的内容管理系统(CMS)。本周，该产品被披露存在 SQL 注入和跨站脚本漏洞，攻击者可利用漏洞获取数据库敏感信息或进行跨站脚本攻击。

CNVD 收录的相关漏洞包括：Joomla! Saxum Picker 组件 SQL 注入漏洞、Joomla! OS Property Real Estate SQL 注入漏洞、Joomla! Kubik-Rubik Simple Image Gallery Extended 跨站脚本漏洞、Joomla! JTicketing 组件 SQL 注入漏洞、Joomla! Jimtawl 任意文件上传漏洞、Joomla! Ek Rishta SQL 注入漏洞、Joomla! CheckList SQL 注入漏洞、Joomla! Alexandria Book Library 组件 SQL 注入漏洞。除“Joomla! Kubik-Rubik Simple Image Gallery Extended 跨站脚本漏洞”外，其余漏洞的综合评级为“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-2018-06166>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05821>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05945>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-06168>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05583>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05951>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05822>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05950>

4、Linux 产品安全漏洞

Linux kernel 是美国 Linux 基金会发布的开源操作系统 Linux 所使用的内核。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞提升权限、读取任意文件或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Linux kernel bnx2x network card 驱动程序拒绝服务漏洞、Linux kernel fs/f2fs/extent_cache.c 文件拒绝服务漏洞、Linux kernel 'futex_request'函数拒绝服务漏洞、Linux kernel NFS server (nfsd) 文件读取漏洞、Linux kernel 'setup_ntlmv2_rsp()'函数空指针解引用漏洞、Linux kernel 本地权限提升漏洞（CNVD-2018-06116）。其中“Linux kernel bnx2x network card 驱动程序拒绝服务漏洞、Linux kernel 'setup_ntlmv2_rsp()'函数空指针解引用漏洞”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-2018-05767>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05820>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05681>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05765>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-06157>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-06116>

5、D-Link DCS-933L 和 DCS-934L 权限获取漏洞

D-Link DCS-933L 和 DCS-934L 都是友讯（D-Link）公司的网络摄像机产品。本周，D-Link 被披露存在权限获取漏洞，攻击者可利用该漏洞获取凭证并控制摄像机。目前，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-2018-05967>

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>

表 4 部分重要高危漏洞列表

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2018-05560	boot2docker 跨站请求伪造漏洞	高	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页： http://boot2docker.io/
CNVD-2018-05561	boot2docker 代码执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页： http://boot2docker.io/
CNVD-201	CloudMe 缓冲区溢出漏洞	高	厂商已发布漏洞修复程序，请及时关

8-05698			注更新： https://www.cloudme.com/zh/sync
CNVD-2018-05872	Stremio Subtitles 远程代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： https://www.strem.io
CNVD-2018-05946	Amazon Music Player 远程代码执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页： https://www.amazon.com/
CNVD-2018-05971	Volkswagen Customer-Link App 和 HTC Customer-Link Bridge 注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页： http://www.vw.com/
CNVD-2018-06019	Geutebruck IP Cameras 远程代码执行漏洞	高	用户可联系供应商获得补丁信息： https://www.geutebrueck.com//en_EN/login.html
CNVD-2018-06094	多款 EMC 产品权限提升漏洞	高	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页： https://www.emc.com
CNVD-2018-06093	多款 Dell 产品任意文件上传漏洞	高	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页： https://www.emc.com
CNVD-2018-06168	Joomla! JTicketing 组件 SQL 注入漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： https://techjoomla.com/

小结：本周，Google 被披露存在权限提升漏洞，攻击者可利用漏洞提升权限。此外，Microsoft、Linux、Joomla!等多款产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码、提升权限或发起拒绝服务攻击等。另外，D-Link 被披露存在权限获取漏洞，攻击者可利用该漏洞获取凭证并控制摄像机。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. Geutebrück 网络摄像头被曝多个高危漏洞

德国 Geutebrück 网络摄像头被曝多个漏洞，但研究人员怀疑其它厂商的网络摄像头也在使用同样的固件，也可能受这些漏洞威胁。虽然路由器、网络摄像头和其它智能设备的安全漏洞不少，但这次漏洞较为严重，所有漏洞评分均介于 8.3-9.8 分区间，属于高危漏洞。德国工业控制系统网络应急响应小组（简称 ICS-CERT）的专家评估这些漏洞表示，这些漏洞可通过互联网被远程利用，即便是低技能的黑客也能加以利用。研究人员目前只能证实这些漏洞影响了 Geutebrück G-Cam/EFD-2250 和 Topline TopF D-2125 网络摄像头。这两款产品均已停产，但 Geutebrück 为此已针对较新的 G-Cam 系列产品发布了固件版本 1.12.0.19，以修复漏洞。。

参考链接: <https://www.easyaq.com/news/798006744.shtml>

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: 010-82991537