# 国家信息安全漏洞共享平台(CNVD)

# 信息安全漏洞周报

2018 年 4 月 16 日-2018 年 4 月 22 日　　2018 年第 16 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**高**。

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 248 个，其中高危漏洞 80 个、中危漏洞 151 个、低危漏洞 17 个。漏洞平均分值为 5.85。本周收录的漏洞中，涉及 0day 漏洞 51 个（占 21%），其中互联网上出现“Secutech RiS-11、RiS-22 和 RiS-33 DNS 更改漏洞、Frog CMS 任意文件上传漏洞”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 695 个，与上周（581 个）环比增长 20%。

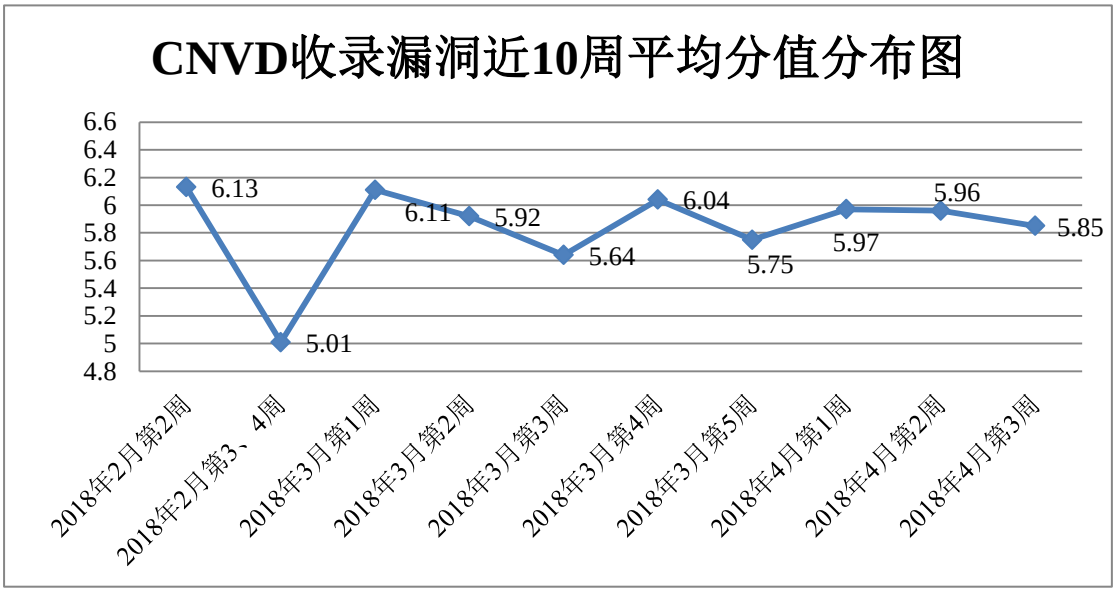


图 1 CNVD 收录漏洞近 10 周平均分值分布图

## 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、哈尔滨安天科技股份有限公司、华为技术有限公司、新华三技术有限公司、北京神州绿盟科技有限

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）、山石网科通信技术有限公司、中新网络信息安全股份有限公司、安徽锋刃信息科技有限公司、北京同余科技有限公司、南瑞集团公司（国网电力科学研究院）、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 695 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 509 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 |
|---|---|---|
| 漏洞盒子 | 360 | 360 |
| 北京天融信网络安全技术有限公司 | 219 | 8 |
| 哈尔滨安天科技股份有限公司 | 202 | 0 |
| 华为技术有限公司 | 157 | 0 |
| 360 网神（补天平台） | 149 | 149 |
| 新华三技术有限公司 | 117 | 0 |
| 北京神州绿盟科技有限公司 | 109 | 0 |
| 北京数字观星科技有限公司 | 95 | 0 |
| 中国电信集团系统集成有限责任公司 | 87 | 0 |
| 北京无声信息技术有限公司 | 16 | 0 |
| 恒安嘉新(北京)科技股份公司 | 13 | 0 |
| 北京知道创宇信息技术有限公司 | 2 | 0 |
| 蓝盾信息安全技术有限公司 | 1 | 1 |
| 沈阳东软系统集成工程有限公司 | 1 | 1 |
| 四川虹微技术有限公司（子午攻防实验室） | 24 | 24 |
| 山石网科通信技术有限公司 | 16 | 16 |
| 中新网络信息安全股份有限公司 | 10 | 10 |

| | | |
|---|---|---|
| 安徽锋刃信息科技有限公司 | 7 | 7 |
| 北京同余科技有限公司 | 1 | 1 |
| 南瑞集团公司（国网电力科学研究院） | 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 广东分中心 | 4 | 4 |
| CNCERT 浙江分中心 | 4 | 4 |
| CNCERT 贵州分中心 | 3 | 3 |
| CNCERT 吉林分中心 | 2 | 2 |
| CNCERT 宁夏分中心 | 2 | 2 |
| 个人 | 86 | 86 |
| 报送总计 | 1704 | 695 |

## 本周漏洞按类型和厂商统计

本周，CNVD 收录了 248 个漏洞。其中应用程序漏洞 139 个，操作系统漏洞 40 个，WEB 应用漏洞 36 个，网络设备漏洞 26 个，安全产品漏洞 7 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 | 139 |
| 操作系统漏洞 | 40 |
| WEB 应用漏洞 | 36 |
| 网络设备漏洞 | 26 |
| 安全产品漏洞 | 7 |

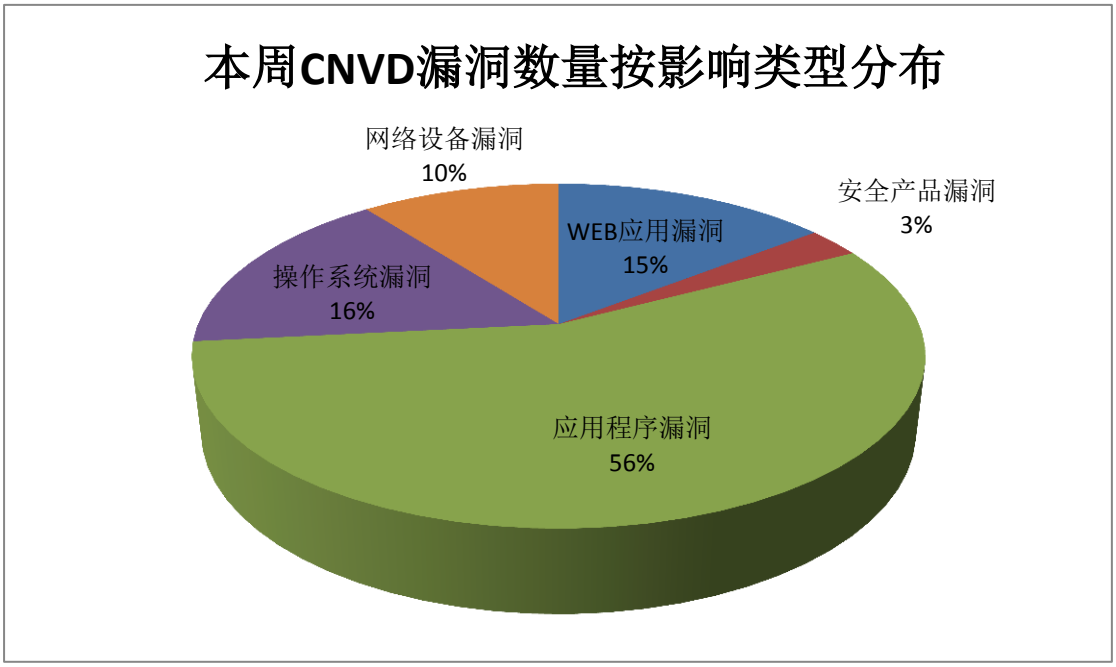


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Microsoft、Google、Wireshark 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 | 18 | 7% |
| 2 | Google | 15 | 6% |
| 3 | Wireshark | 14 | 6% |
| 4 | Huawei | 12 | 5% |
| 5 | Apple | 10 | 4% |
| 6 | AMD | 7 | 3% |
| 7 | IBM | 7 | 3% |
| 8 | Cisco | 6 | 2% |
| 9 | Mitel | 6 | 2% |
| 10 | 其他 | 153 | 62% |

## 本周行业漏洞收录情况

本周，CNVD 收录了 11 个电信行业漏洞，29 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，“Huawei 多个 AR 系列产品拒绝服务漏洞、Oracle WebLogic Server WLS 核心组件反序列化漏洞、Moxa EDR-810 命令注入漏洞、Google And

roid 权限提升漏洞（CNVD-2018-07850）、LCDS LAquis SCADA 任意代码执行漏洞”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/

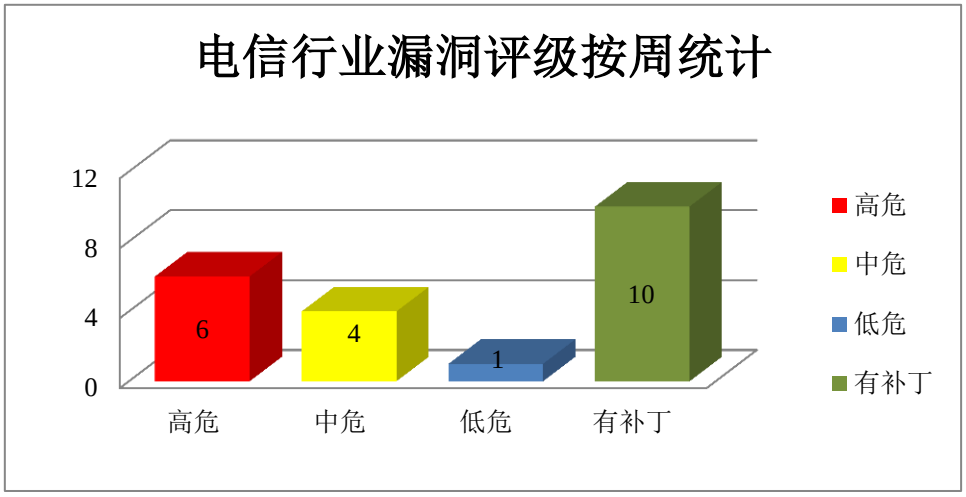


图 3 电信行业漏洞统计

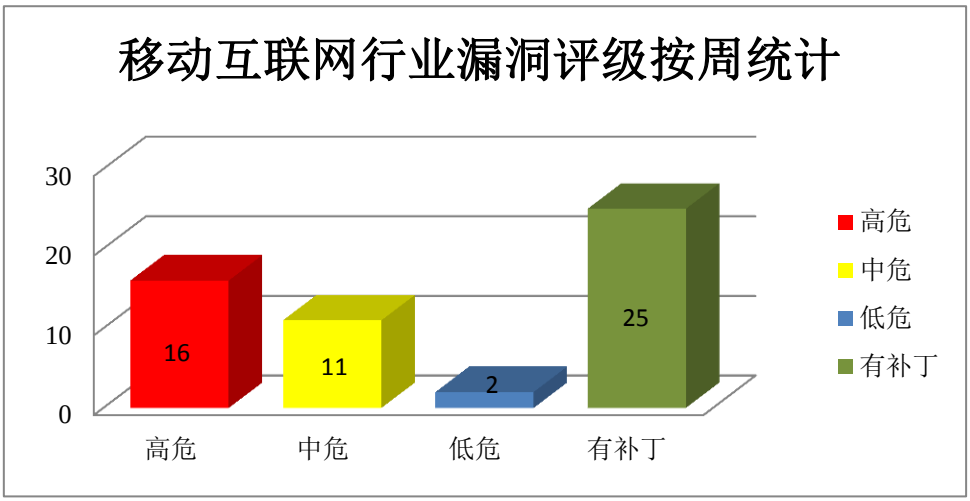


图 4 移动互联网行业漏洞统计

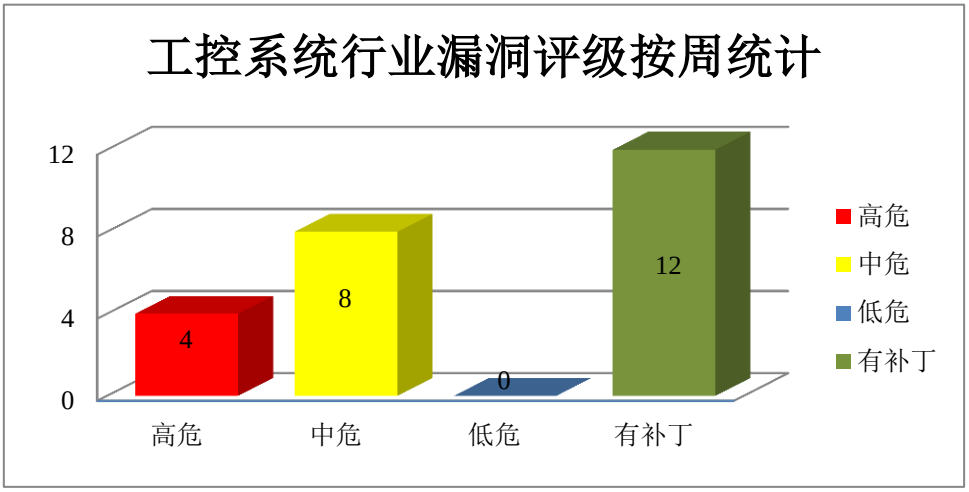


图 5 工控行业漏洞统计

## 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、WebLogic Server WLS 核心组件反序列化漏洞

WebLogic Server 是美国甲骨文（Oracle）公司开发的一款适用于云环境和传统环境的应用服务中间件。本周，该产品被披露存在反序列化漏洞，攻击者可利用漏洞在未授权的情况下远程执行代码。

CNVD 收录的相关漏洞包括：Oracle WebLogic Server WLS 核心组件反序列化漏洞。该漏洞的综合评级为“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-2018-07811

### 2、Apple 产品安全漏洞

Apple iOS 是为移动设备所开发的一套操作系统；Safari 是一款 Web 浏览器，是 Mac OS X 和 iOS 操作系统附带的默认浏览器。iCloud for Windows 是一款基于 Windows 平台的云服务。WebKit 是其中的一个 Web 浏览器引擎组件。本周，上述产品被披露存在内存破坏漏洞，攻击者可利用漏洞执行任意代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：多款 Apple 产品 WebKit 内存破坏漏洞（CNVD-2018-07779、CNVD-2018-07780、CNVD-2018-07781、CNVD-2018-07782、CNVD-2018-07807、CNVD-2018-07808、CNVD-2018-07809、CNVD-2018-07810）。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-2018-07779

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07780

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07781

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07782

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07807

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07808

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07809

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07810

### 3、Google 产品安全漏洞

Android 是美国谷歌（Google）公司和开放手持设备联盟（简称 OHA）共同开发的一套以 Linux 为基础的开源操作系统。Qualcomm closed-source components 是其中的一个美国高通（Qualcomm）公司开发的闭源组件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏提升权限或执行任意代码等。

CNVD 收录的相关漏洞包括：Google Android 本地权限提升漏洞（CNVD-2018-07851、CNVD-2018-07863）、Google Android 缓冲区溢出漏洞（CNVD-2018-07849、CNVD-2018-07861）、Google Android 权限提升漏洞（CNVD-2018-07850、CNVD-2018-07858）、Google Android 远程代码执行漏洞（CNVD-2018-07862）、Google Android Qualcomm 闭源组件缓冲区溢出漏洞。除“Google Android 本地权限提升漏洞（CNVD-2018-07851、CNVD-2018-07863）”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-2018-07851

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07863

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07849

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07861

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07850

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07858

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07862

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07765

### 4、Microsoft 产品安全漏洞

Microsoft Windows 10 和 Windows Server 2016 都是美国微软（Microsoft）公司的产品。Edge 是其中的一个系统附带的默认浏览器。Internet Explorer（IE）是一款 Windows 操作系统附带的 Web 浏览器。本周，上述产品被披露存在远程代码执行漏洞，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 ChakraCore 和 Edge 远程代码执行漏洞（CNVD-2018-07772、CNVD-2018-07773、CNVD-2018-07774、CNVD-2018-07775）、Microsoft Internet Explorer 远程代码执行漏洞（CNVD-2018-07776、CNVD-2018-07777、CNVD-2018-07778、CNVD-2018-08022）。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-2018-07772
http://www.cnvd.org.cn/flaw/show/CNVD-2018-07773
http://www.cnvd.org.cn/flaw/show/CNVD-2018-07774
http://www.cnvd.org.cn/flaw/show/CNVD-2018-07775
http://www.cnvd.org.cn/flaw/show/CNVD-2018-07776
http://www.cnvd.org.cn/flaw/show/CNVD-2018-07777
http://www.cnvd.org.cn/flaw/show/CNVD-2018-07778
http://www.cnvd.org.cn/flaw/show/CNVD-2018-08022

### 5、MikroTik RouterOS 权限提升漏洞

MikroTik RouterOS 是拉脱维亚 MikroTik 公司的一套基于 Linux 核心开发的路由操作系统。本周，MikroTik 被披露存在权限提升漏洞，远程攻击者可利用该漏洞获取客户端内部网络的访问权限。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-2018-07908

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-2018-07712 | Mozilla Firefox 代码执行漏洞（CNVD-2018-07712） | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://www.mozilla.org/en-US/security/advisories/mfsa2018-10/ |
| CNVD-2018-07715 | Dell EMC Isilon OneFS 不正确授权漏洞 | 高 | 厂商已发布漏洞修复程序，请及时关注更新：https://support.emc.com/downloads/15209_Isilon-OneFS |
| CNVD-2018-07716 | Jolokia agent JNDI 注入漏洞 | 高 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://jolokia.org/#Security_fixes_with_1.5.0 |
| CNVD-2018-07745 | LCDS LAquis SCADA 任意代码执行漏洞 | 高 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://laquisscada.com/instale1.php |
| CNVD-2018-07756 | textpattern 拒绝服务漏洞 | 高 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/textpattern/textpatter |

| | | | |
|---|---|---|---|
| | | | n/issues/1098 |
| CNVD-2018-07865 | Moxa EDR-810 命令注入漏洞 | 高 | 用户可联系供应商获得补丁信息：https://www.moxa.com/support/download.aspx?type=support&id=15851 |
| CNVD-2018-07880 | Heimdal PRO 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://heimdalsecurity.com/ |
| CNVD-2018-07879 | Heimdal PRO 文件执行漏洞 | 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://heimdalsecurity.com/ |
| CNVD-2018-07893 | Mitel ST conferencing 组件文件上传漏洞 | 高 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.mitel.com/mitel-product-security-advisory-18-0004 |
| CNVD-2018-07948 | Mitel Connect ONSITE 和 Mitel ST conferencing 组件 PHP 漏洞 | 高 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.mitel.com/mitel-product-security-advisory-18-0004 |

小结：本周，Oracle WebLogic Server 被披露存在反序列化漏洞，攻击者可利用漏洞在未授权的情况下远程执行代码。此外，Apple、Google、Microsoft 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，MikroTik 被披露存在权限提升漏洞，远程攻击者可利用该漏洞获取客户端内部网络的访问权限。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. Moxa 工业路由器曝 17 项漏洞

思科旗下 Talos 情报与研究小组报告称，其共在 Moxa （摩莎）公司的工业路由器当中发现 17 项安全漏洞，其中包括多种高危的命令注入与拒绝服务（DoS）漏洞。这些安全漏洞源自 Moxa EDR-810 设备，该设备是一台集成化工业多端口安全路由器，可提供防火墙、NAT、VPN 以及托管二层交换机功能。思科公司发现的这几项问题已经被定性为可对 Moxa 路由器的 Web 服务功能产生影响的高危命令注入漏洞。这些漏洞允许攻击者通过向目标设备发送特定的 HTTP POST 请求以提升权限，并以此获取目标系统上的 root shell。上述问题于 2017 年 11 月中下旬上报至 Moxa 公司处，2018 年 4 月 12 日该公司发布的 Moxa EDR-810 v4.1 中已对这些漏洞进行了修复。

参考链接：https://www.easyaq.com/news/1079417823.shtml

### 2. LG 网络存储设备曝严重 RCE 漏洞

LG NAS 设备是连接到网络的专用文件存储单元，允许用户使用多台计算机来存储

和共享数据。VPN Mentor 的研究人员表示，尽管无法通过随意输入的用户名和密码来登陆 LG NAS 设备，但他们发现大多数 LG NAS 设备中都存在一个 pre-auth 远程命令注入漏洞。漏洞来源于远程管理用户登录页面的“密码”参数的错误验证方式，允许远程攻击者通过密码字段传递任意系统命令。由于 LG 公司尚未发布针对此漏洞的修复程序，因此我们建议 LG NAS 设备用户应确保自己的设备无法通过公共互联网访问，并使用防火墙来对其进行保护。

参考链接：https://www.easyaq.com/news/801883123.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