国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2018 年 2 月 26 日-2018 年 3 月 4 日 **2018 年第 9 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 397 个，其中高危漏洞 144 个、中危漏洞 219 个、低危漏洞 34 个。漏洞平均分值为 6.11。本周收录的漏洞中，涉及 0day 漏洞 62 个（占 16%），其中互联网上出现“iBall iB-WRA150N 远程代码执行漏洞、D-Link DSL-2640U 和 DSL-2540U 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 679 个。

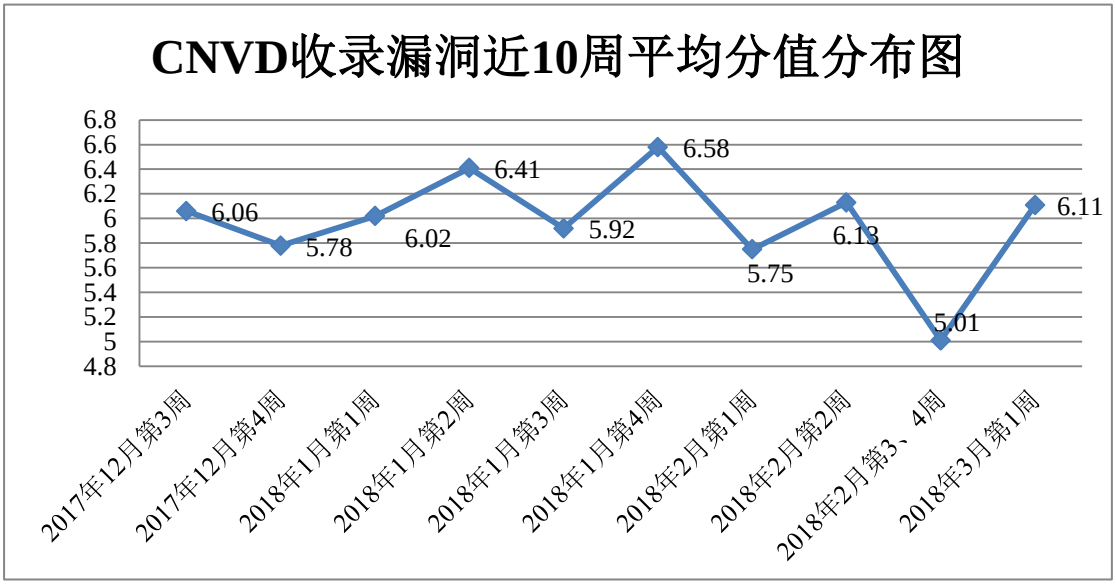

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，蓝盾信息安全技术有限公司、北京天融信网络安全技术有限公司、东软、北京启明星辰信息安全技术有限公司、恒安嘉新(北京)科技股份公司、哈尔滨安天科技股份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）、南瑞集团公司（国网电力科学研究院）、南京联成科技发展股份有限公司、中新网络信息安全股份有限公司、福建省海峡信息技术有限公司、常州瑞新网络科技股份有限公司、北京智游网安科技有限公司、北京同余科技有限公司、漏斗社区及其他个人白帽子向 CNVD 提交了 679 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 288 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
蓝盾信息安全技术有限公司	750	0
北京天融信网络安全技术有限公司	298	1
360 网神（补天平台）	280	280
东软	271	2
北京启明星辰信息安全技术有限公司	238	0
恒安嘉新(北京)科技股份公司	194	0
哈尔滨安天科技股份有限公司	166	0
华为技术有限公司	96	0
中国电信集团系统集成有限责任公司	78	1
新华三技术有限公司	73	0
北京神州绿盟科技有限公司	69	0
卫士通信息产业股份有限公司	40	0
漏洞盒子	8	8
北京数字观星科技有限公司	6	0
北京无声信息技术有限公司	5	0
知道创宇	1	0
四川虹微技术有限公司（子午攻防实验室）	46	46

南瑞集团公司（国网电力科学研究院）	26	26
南京联成科技发展股份有限公司	16	16
中新网络信息安全股份有限公司	12	12
福建省海峡信息技术有限公司	11	11
常州瑞新网络科技股份有限公司	2	2
北京智游网安科技有限公司	2	2
北京同余科技有限公司	1	1
漏斗社区	1	1
CNCERT 重庆分中心	23	23
CNCERT 上海分中心	20	20
CNCERT 江西分中心	10	10
CNCERT 湖南分中心	7	7
CNCERT 山西分中心	6	6
CNCERT 天津分中心	6	6
CNCERT 宁夏分中心	5	5
CNCERT 广东分中心	5	5
CNCERT 贵州分中心	2	2
CNCERT 四川分中心	2	2
CNCERT 吉林分中心	1	1
CNCERT 安徽分中心	1	1
CNCERT 新疆分中心	1	1
CNCERT 浙江分中心	1	1
个人	180	180

报送总计	2960	679

本周漏洞按类型和厂商统计

本周，CNVD 收录了 397 个漏洞。其中应用程序漏洞 267 个，WEB 应用漏洞 45 个，网络设备漏洞 37 个，操作系统漏洞 28 个，安全产品漏洞 10 个，数据库漏洞 10 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	267
WEB 应用漏洞	45
网络设备漏洞	37
操作系统漏洞	28
安全产品漏洞	10
数据库漏洞	10

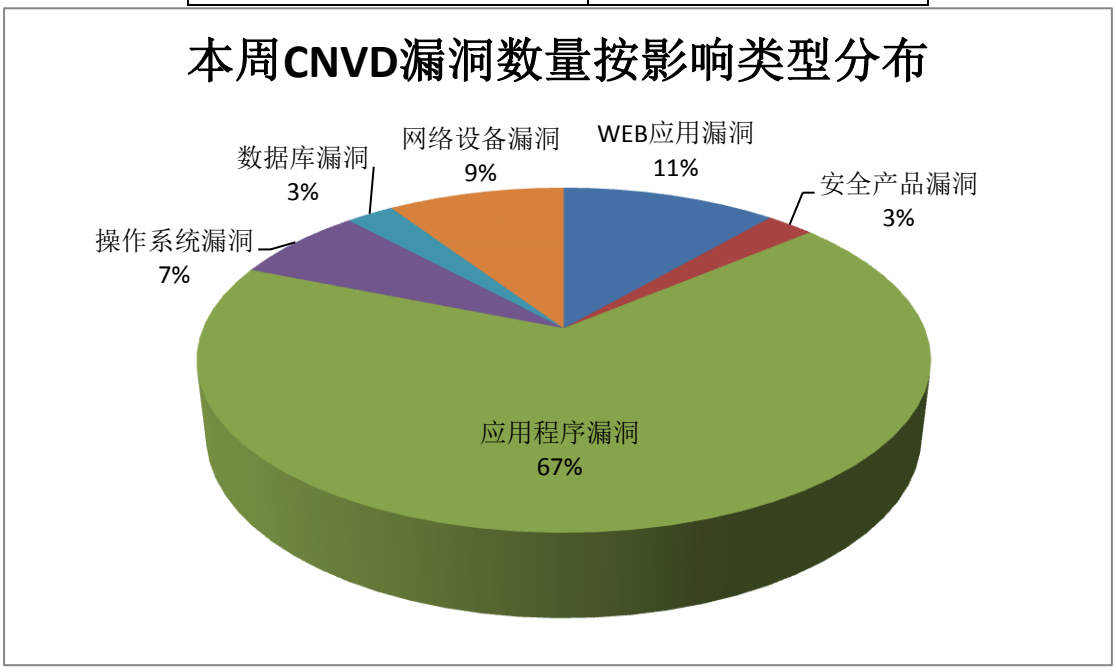

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、IBM、Microsoft 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	Google	41	10%
2	IBM	22	6%
3	Microsoft	21	5%

4	Blender	21	5%
5	Apache	17	4%
6	HP	14	4%
7	PHP Scripts Mall	13	3%
8	CCN-lite	10	3%
9	CloudBees	9	2%
10	其他	229	58%

本周行业漏洞收录情况

本周，CNVD 收录了 29 个电信行业漏洞，31 个移动互联网行业漏洞，14 个工控行业漏洞（如下图所示）。其中，“多款 Apple 产品 Audio 内存破坏漏洞、Google Android libmediadrm 权限提升漏洞、BUFFALO WXR-1900DHP2 身份验证漏洞、Apache Tomcat 代码执行漏洞、Moxa OnCell G3100-HSPA Series 拒绝服务漏洞”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/

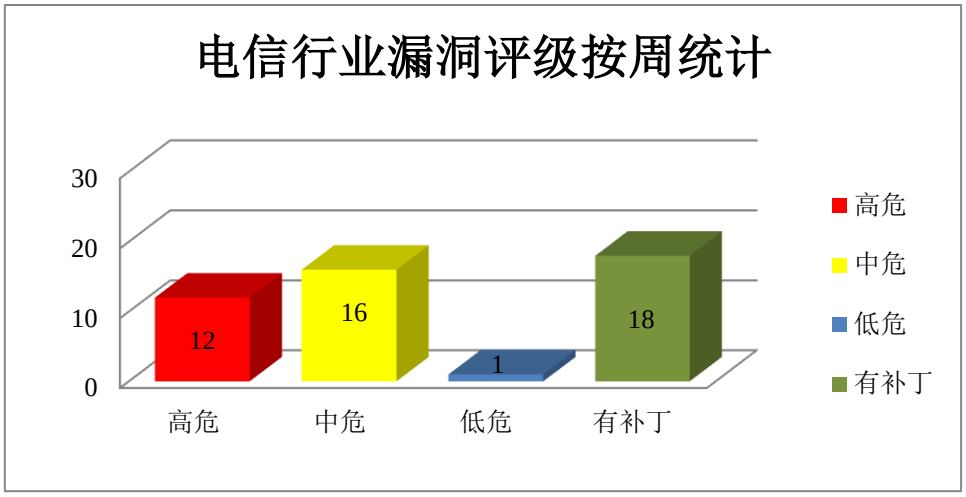

图 3 电信行业漏洞统计

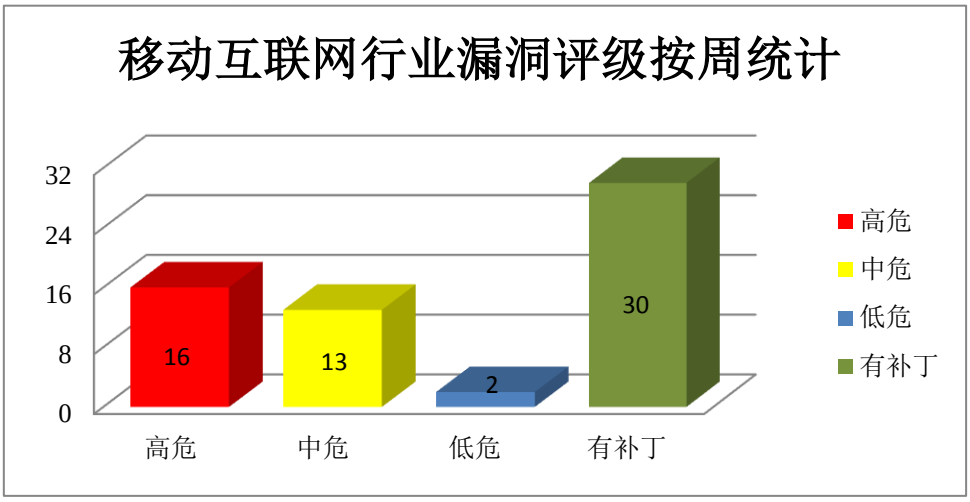

图 4 移动互联网行业漏洞统计

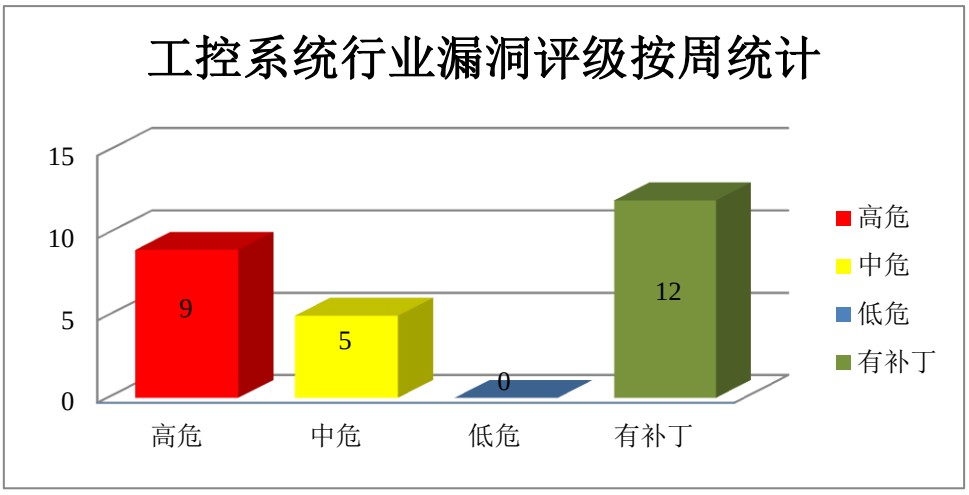

图 5 工控行业漏洞统计

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、Microsoft 产品安全漏洞

Microsoft Windows 是美国微软（Microsoft）公司发布的一系列操作系统。Edge 是其中的一个系统附带的浏览器。ChakraCore 是使用在 Edge 的一个开源的 JavaScript 引擎的核心部分。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。

CNVD 收录的相关漏洞包括：Microsoft Edge 和 ChakraCore 远程内存破坏漏洞（CNVD-2018-03513、CNVD-2018-03514、CNVD-2018-03515、CNVD-2018-03519、CNVD-2018-03520、CNVD-2018-03521、CNVD-2018-03522、CNVD-2018-03523）。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-2018-03513
http://www.cnvd.org.cn/flaw/show/CNVD-2018-03514
http://www.cnvd.org.cn/flaw/show/CNVD-2018-03515
http://www.cnvd.org.cn/flaw/show/CNVD-2018-03519
http://www.cnvd.org.cn/flaw/show/CNVD-2018-03520
http://www.cnvd.org.cn/flaw/show/CNVD-2018-03521
http://www.cnvd.org.cn/flaw/show/CNVD-2018-03522
http://www.cnvd.org.cn/flaw/show/CNVD-2018-03523

2、Apache 产品安全漏洞

Apache Geode 是美国阿帕奇软件基金会的一套应用于分布式云架构中提供对数据密集型应用程序实时和一致访问数据的管理平台。Apache Thrift 是一套远程调用框架。Apache Ranger 是一套为 Hadoop 集群实现全面安全措施的架构。Tomcat 是 Jakarta 项目开发的一个 Servlet 容器。本周，上述产品被披露存在安全绕过和代码执行漏洞，攻击者可利用漏洞绕过安全限制或执行任意代码。

CNVD 收录的相关漏洞包括：Apache Geode 代码执行漏洞（CNVD-2018-04075、CNVD-2018-04076）、Apache Ranger 安全绕过漏洞（CNVD-2018-03764）、Apache Thrift Go client 库远程代码执行漏洞、Apache Tomcat 安全绕过漏洞（CNVD-2018-03661、CNVD-2018-03662）、Apache Tomcat 代码执行漏洞、Apache Ranger 安全绕过漏洞。除“Apache Ranger 安全绕过漏洞”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-2018-04075
http://www.cnvd.org.cn/flaw/show/CNVD-2018-04076
http://www.cnvd.org.cn/flaw/show/CNVD-2018-03764
http://www.cnvd.org.cn/flaw/show/CNVD-2018-03760
http://www.cnvd.org.cn/flaw/show/CNVD-2018-03661
http://www.cnvd.org.cn/flaw/show/CNVD-2018-03662
http://www.cnvd.org.cn/flaw/show/CNVD-2018-03757
http://www.cnvd.org.cn/flaw/show/CNVD-2018-03763

3、Google 产品安全漏洞

Google Chrome for Mac、Windows 和 Linux 是美国谷歌公司开发的一款基于 Mac、Windows 和 Linux 平台的 Web 浏览器。Qualcomm WLAN driver 是其中的一个无线驱动程序。Qualcomm Graphics_Linux 是一个基于 Linux 系统的图形组件。libmediadrm 是其中的一个 DRM 数字版权管理库。本周，上述产品被披露存在安全绕过和权限提升漏洞，攻击者可利用漏洞绕过安全限制或提升权限。

CNVD 收录的相关漏洞包括：Google Chrome for Mac、Windows 和 Linux 安全绕过漏洞（CNVD-2018-03636、CNVD-2018-03631、CNVD-2018-03790、CNVD-2018-03794、CNVD-2018-03797）、Google Android libmediadrm 权限提升漏洞、Google Android Qualcomm Graphics_Linux 组件权限提升漏洞、Google Android Qualcomm WLAN 组件权限提升漏洞。其中，“Google Android libmediadrm 权限提升漏洞、Google Android Qualcomm Graphics_Linux 组件权限提升漏洞、Google Android Qualcomm WLAN 组件权限提升漏洞”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-2018-03636

http://www.cnvd.org.cn/flaw/show/CNVD-2018-03631

http://www.cnvd.org.cn/flaw/show/CNVD-2018-03790

http://www.cnvd.org.cn/flaw/show/CNVD-2018-03794

http://www.cnvd.org.cn/flaw/show/CNVD-2018-03797

http://www.cnvd.org.cn/flaw/show/CNVD-2018-03827

http://www.cnvd.org.cn/flaw/show/CNVD-2018-03819

http://www.cnvd.org.cn/flaw/show/CNVD-2018-03821

4、IBM 产品安全漏洞

IBM Client Application Access 和 IBM Notes 都是美国 IBM 公司的产品。IBM Client Application Access 是一套用来访问本地应用程序的工具。IBM Notes 是一套协同办公软件。IBM Runtimes for Java Technology 是一套运行 Java 程序的运行时环境。IBM WebSphere MQ 是的一款消息传递中间件产品。本周，上述产品被披露存在信息泄露和权限提升漏洞，攻击者可利用漏洞泄露敏感信息或提升权限。

CNVD 收录的相关漏洞包括：IBM Client Application Access 和 Notes 权限提升漏洞、IBM Client Application Access 和 Notes 权限提升漏洞（CNVD-2018-03879）、IBM Client Application Access 权限提升漏洞、IBM Client Application Access 权限提升漏洞（CNVD-2018-03867、CNVD-2018-03868、CNVD-2018-03876）、IBM Runtimes for Java Technology J9 JVM 权限提升漏洞、IBM WebSphere MQ GSKit 信息泄露漏洞。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-2018-03878

http://www.cnvd.org.cn/flaw/show/CNVD-2018-03879

http://www.cnvd.org.cn/flaw/show/CNVD-2018-03875

http://www.cnvd.org.cn/flaw/show/CNVD-2018-03867

http://www.cnvd.org.cn/flaw/show/CNVD-2018-03868

http://www.cnvd.org.cn/flaw/show/CNVD-2018-03876

http://www.cnvd.org.cn/flaw/show/CNVD-2018-03877

http://www.cnvd.org.cn/flaw/show/CNVD-2018-03885

5、iBall iB-WRA150N 远程代码执行漏洞

iBall iB-WRA150N 是印度 iBall 公司的一款无线路由器产品。本周，iBall 被披露存在远程代码执行漏洞，远程攻击者可借助 Diagnostics 页面中因特网包探索器（PING）检测参数的 shell 元字符利用该漏洞执行操作系统命令。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-2018-04192

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-2018-03679	CCN-lite 越界访问漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://github.com/cn-uofbasel/ccn-lite/releases/tag/2.0.0
CNVD-2018-03682	CCN-lite 缓冲区溢出漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://github.com/cn-uofbasel/ccn-lite/releases/tag/2.0.0
CNVD-2018-03683	CCN-lite 整数溢出漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://github.com/cn-uofbasel/ccn-lite/releases/tag/2.0.0
CNVD-2018-03785	Quest NetVault Backup 任意代码执行漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://zerodayinitiative.com/advisories/ZDI-18-004/
CNVD-2018-03784	Quest NetVault Backup 拒绝服务漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://zerodayinitiative.com/advisories/ZDI-18-005/
CNVD-2018-03786	Vobot Clock 信息泄露漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：http://stacksmashing.net/CVE-2018-6827.html
CNVD-2018-03788	Vobot Clock root 权限硬编码 SSH 凭证漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：http://stacksmashing.net/CVE-2018-6825.html

CNVD-2018-03787	Vobot Clock 远程代码执行漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：http://stacksmashing.net/CVE-2018-6826.html
CNVD-2018-03811	Philips Intellispace Porta 本地权限提升漏洞	高	用户可联系供应商获得补丁信息：http://incenter.medical.philips.com
CNVD-2018-03812	Philips Intellispace Portal 权限提升漏洞	高	用户可联系供应商获得补丁信息：http://incenter.medical.philips.com

小结：本周，Microsoft 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。此外，Apache、Google、IBM 等多款产品被披露存在多个漏洞，攻击者可利用漏洞执行信息泄露、安全绕过或提升权限等。另外，iBall 被披露存在远程代码执行漏洞，远程攻击者可借助 Diagnostics 页面中因特网包探索器（PING）检测参数的 shell 元字符利用该漏洞执行操作系统命令。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. Github 遭遇史上最大 1.35 Tbps DDoS 攻击

最大代码分发平台 Github 在周三遭受了一系列大规模分布式拒绝服务（DDoS）攻击。在攻击的第一阶段，Github 的网站遭受了惊人的每秒 1.35 太比特（Tbps）的高峰，而在第二阶段，Github 的网络监控系统检测到了 400Gbps 的峰值。攻击持续了 8 分钟以上，并且由于攻击使用了大量流量，这是迄今为止见过的最大的 DDoS 攻击。此前，法国电信 OVH 和 Dyn DNS 遭遇了 1 Tbps 流量的 DDoS 攻击。两起攻击都是黑客利用 Mirai 进行的，Mirai 是一种感染物联网设备进行大规模 DDoS 攻击的病毒。然而，就 Github 而言，大规模攻击时源于 Akamai，Arbor Networks 和 Cloudflare 的 Memcached 服务器中的严重安全漏洞。据研究人员介绍，Memcached 服务器的 UDP 协议的实现存在漏洞，可以被用来发起重大的 DDoS 攻击。

参考链接：http://www.freebuf.com/news/164009.html

2. SAML 漏洞：允许攻击者以其他用户身份实现登录

美国网络安全公司 Duo Labs 与美国计算机紧急响应小组协调中心（简称 CERT/CC）的安全研究人员们日前发布安全公告，详尽描述了新的 SAML 安全漏洞。此项漏洞允许恶意攻击者在无需知晓受害者密码内容的前提下以合法用户身份完成登录验证。攻击利用这项安全漏洞的惟一先决条件，在于其需要在受害者网络当中拥有一个注册帐号。通过这种方式，攻击者即可查询 SAML 供应方并伪造请求，从而“作为其他用户进行身份验证，最终骗过 SAML 系统”。

参考链接：https://www.easyaq.com/news/1334142830.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