国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2018 年 12 月 10 日-2018 年 12 月 16 日 **2018 年第 50 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 198 个，其中高危漏洞 71 个、中危漏洞 108 个、低危漏洞 19 个。漏洞平均分值为 5.99。本周收录的漏洞中，涉及 0day 漏洞 29 个（占 15%），其中互联网上出现“Mantis 'manage_proj_page.php' PHP 代码注入漏洞、Tarantella Enterprise 路径遍历漏洞”等代码攻击漏洞。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 1213 个，与上周（987 个）环比增长 23%。

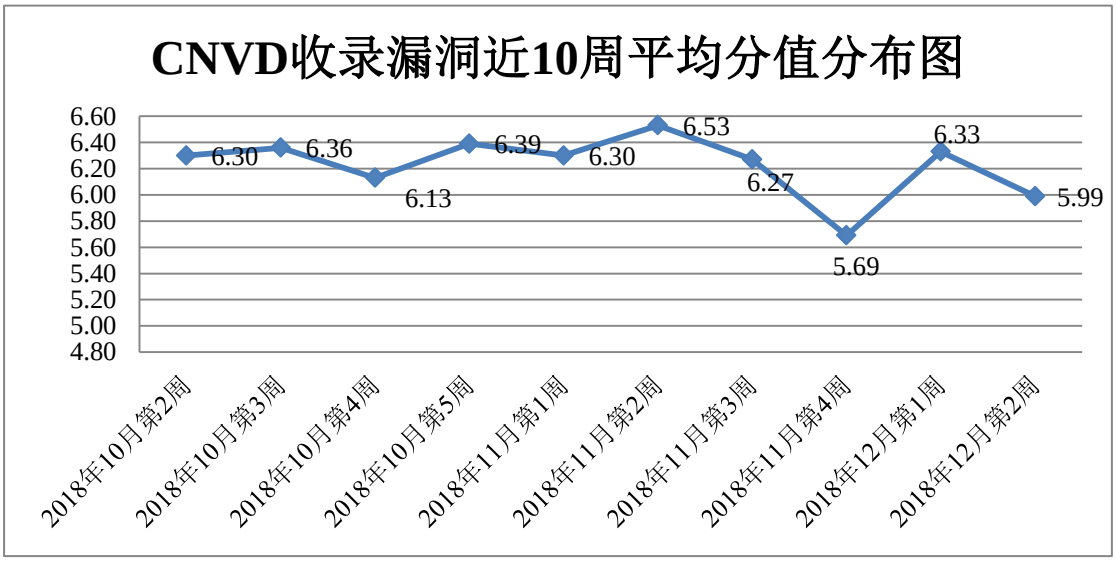

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞事件处置情况

本周，CNVD 向基础电信企业通报漏洞事件 3 起，向银行、保险、能源等重要行业单位通报漏洞事件 13 起，协调 CNCERT 各分中心验证和处置涉及地方重要部门漏洞事件 156 起，协调教育行业应急组织验证和处置高校科研院所系统漏洞事件 88 起，向国

家上级信息安全协调机构上报涉及部委门户、子站或直属单位信息系统漏洞事件14起。

此外，CNVD 通过已建立的联系机制或涉事单位公开联系渠道向以下单位通报了其信息系统或软硬件产品存在的漏洞，具体处置单位情况如下所示：

深圳市皓峰通讯技术有限公司、深圳市锟铻科技有限公司、北京奥博思软件技术有限公司、酷溜网（北京）科技有限公司、济南考源信息科技有限公司、同方知网(北京)技术有限公司、北京百卓网络技术有限公司、洪湖尔创网联信息技术有限公司、哈尔滨伟成科技有限公司、深圳市湛蓝设计有限公司、广州志华软件科技有限公司、漳州豆壳网络科技有限公司、太原国远天成网络科技有限公司、淄博闪灵网络科技有限公司、福州网健天下网络科技有限公司、广东百城人才网络股份有限公司、广东百城人才网络股份有限公司、佛山市杜特软件科技有限公司、成都智汇安新科技有限公司、石家庄灵石科技有限公司、深圳市乔安科技有限公司、云迈电子商务有限公司、长沙德尚网络科技有限公司、ThinkCMF、ZZZCMS、YFCMF、twothink、zzcms、EARCLINK、Seacms、Busybox、ianmi、Adobe、老班 CMS、飞飞影视导航系统（FeiFeiCms）、中国医药保健品进出口商会、平阳县屏鹿软件工作室、中国医药保健品进出口商会。

本周，CNVD 发布了《关于 SQLite 远程代码执行漏洞的安全公告》和《关于 ThinkPHP 存在远程代码执行漏洞的安全公告》。详情参见 CNVD 网站公告内容。

http://www.cnvd.org.cn/webinfo/show/4803

http://www.cnvd.org.cn/webinfo/show/4805

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、新华三技术有限公司、哈尔滨安天科技集团股份有限公司、华为技术有限公司、北京启明星辰信息安全技术有限公司等单位报送公开收集的漏洞数量较多。山东云天安全技术有限公司、上海银基信息安全技术股份有限公司、南京联成科技发展股份有限公司、北京国舜科技股份有限公司、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、北京圣博润高新技术股份有限公司、河南信安世纪科技有限公司、任子行网络技术股份有限公司、广州竞远安全技术股份有限公司、内蒙古奥创科技有限公司、山石网科通信技术有限公司、北京同余科技有限公司及其他个人白帽子向 CNVD 提交了 1213 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）和斗象科技（漏洞盒子）向 CNVD 共享的白帽子报送的 756 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	412	14

360 网神（补天平台）	407	407
斗象科技（漏洞盒子）	349	349
新华三技术有限公司	299	0
哈尔滨安天科技集团股份有限公司	222	0
华为技术有限公司	190	0
北京启明星辰信息安全技术有限公司	108	0
深信服科技股份有限公司	80	0
北京数字观星科技有限公司	79	0
北京神州绿盟科技有限公司	50	0
中国电信集团系统集成有限责任公司	45	2
恒安嘉新(北京)科技股份公司	13	0
深圳市腾讯计算机系统有限公司（玄武实验室）	13	13
北京知道创宇信息技术有限公司	1	0
南京铱迅信息技术股份有限公司	1	1
厦门服云信息科技有限公司	1	1
沈阳东软系统集成工程有限公司	1	1
山东云天安全技术有限公司	57	57
上海银基信息安全技术股份有限公司	48	48
南京联成科技发展股份有限公司	32	32
北京国舜科技股份有限公司	29	29
中新网络信息安全股份有限公司	21	21
安徽锋刃信息科技有限公司	18	18

北京圣博润高新技术股份有限公司	11	11
河南信安世纪科技有限公司	11	11
任子行网络技术股份有限公司	10	10
广州竞远安全技术股份有限公司	4	4
内蒙古奥创科技有限公司	3	3
山石网科通信技术有限公司	1	1
北京同余科技有限公司	1	1
CNCERT 山西分中心	8	8
CNCERT 新疆分中心	8	8
CNCERT 上海分中心	6	6
CNCERT 贵州分中心	2	2
CNCERT 吉林分中心	2	2
CNCERT 宁夏分中心	2	2
CNCERT 甘肃分中心	1	1
CNCERT 天津分中心	1	1
个人	149	149
报送总计	2696	1213

本周漏洞按类型和厂商统计

本周，CNVD 收录了 198 个漏洞。应用程序漏洞 140 个，操作系统漏洞 33 个，网络设备漏洞 15 个，WEB 应用漏洞 7 个，数据库漏洞 2 个，安全产品漏洞 1 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	140
操作系统漏洞	33
网络设备漏洞	15

WEB 应用漏洞	7
数据库漏洞	2
安全产品漏洞	1

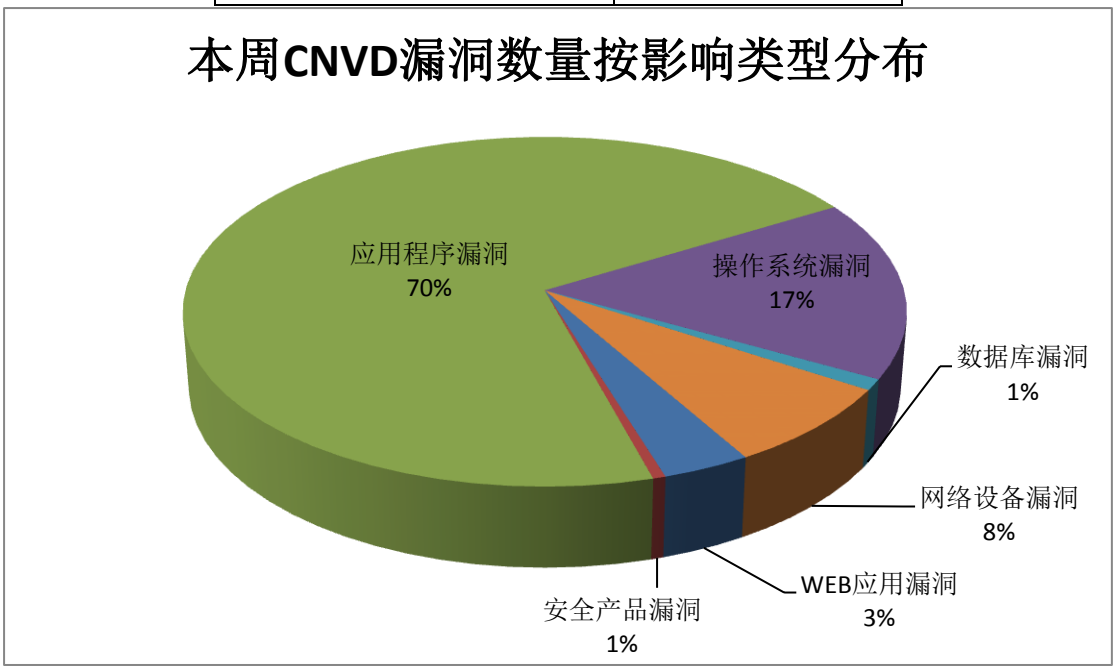

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 IBM、Foxit、Siemens 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	IBM	34	17%
2	Foxit	27	13%
3	Siemens	18	9%
4	Google	15	8%
5	Apple	11	6%
6	Microsoft	11	6%
7	Adobe	10	5%
8	ASUSTOR	8	4%
9	Qualcomm	4	2%
10	其他	60	30%

本周行业漏洞收录情况

本周，CNVD 收录了 2 个电信行业漏洞，8 个移动互联网行业漏洞，27 个工控行业

漏洞（如下图所示）。其中，“Siemens EN100 Ethernet Communication Module 拒绝服务漏洞、Oracle WebLogic Server 存在文件上传漏洞、Siemens SIMATIC S7-400 输入验证漏洞、Google Android 缓冲区溢出漏洞（CNVD-2018-25279）、多款 Siemens 产品远程代码执行漏洞”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/

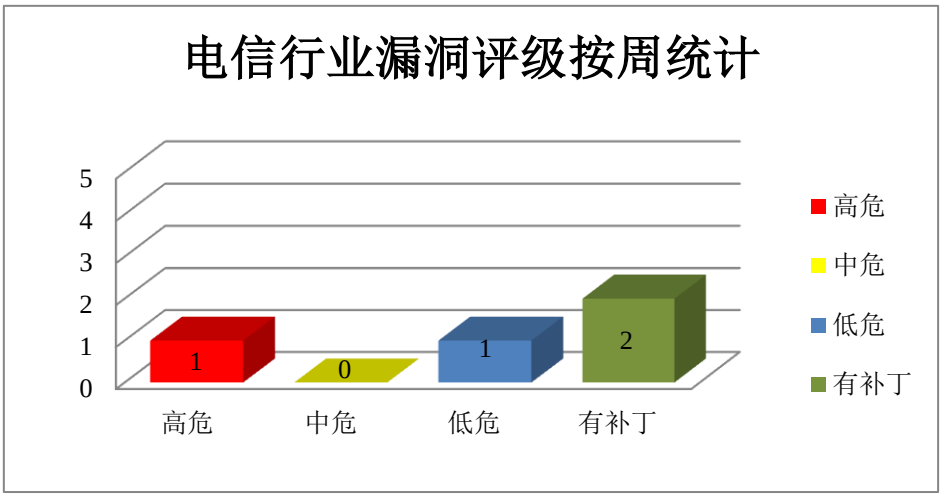

图 3 电信行业漏洞统计

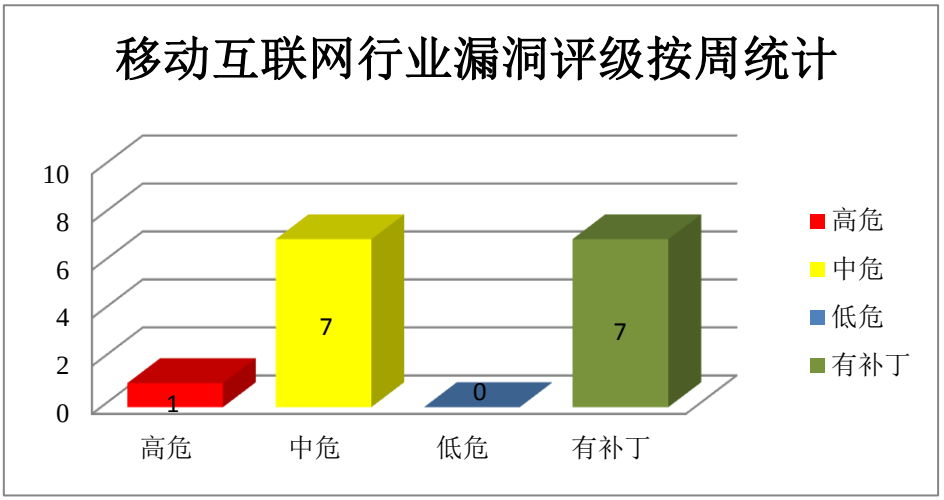

图 4 移动互联网行业漏洞统计

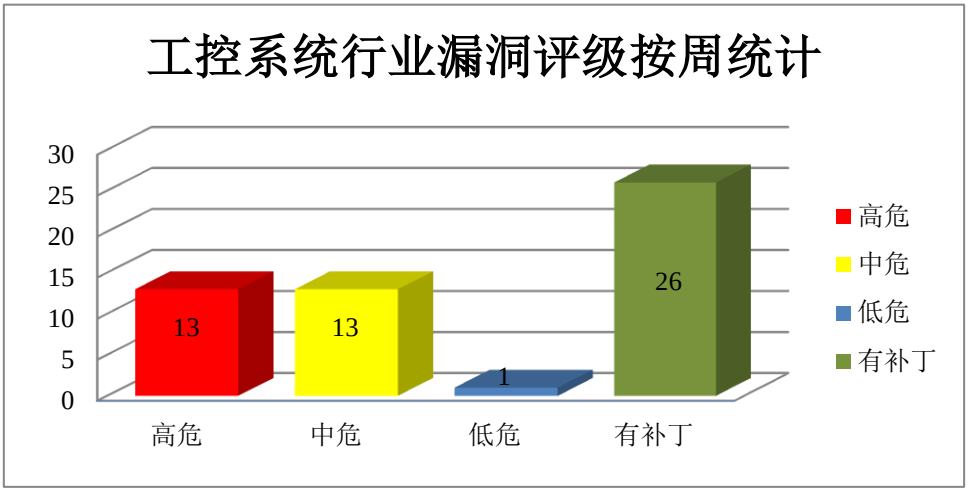

图 5 工控系统行业漏洞统计

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、Foxit 产品安全漏洞

Foxit Reader for Windows 是一款基于 Windows 平台的 PDF 文档阅读器。Foxit PhantomPDF for Windows 是它的商业版。本周，上述产品被披露存在内存错误引用漏洞，攻击者可利用漏洞在当前进程的上下文中执行代码。

CNVD 收录的相关漏洞包括：Foxit Reader 和 Foxit PhantomPDF for Windows 内存错误引用漏洞（CNVD-2018-25189、CNVD-2018-25190、CNVD-2018-25192、CNVD-2018-25193、CNVD-2018-25194、CNVD-2018-25195、CNVD-2018-25196、CNVD-2018-25197）。上述漏洞的综合评级为为“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-2018-25189

http://www.cnvd.org.cn/flaw/show/CNVD-2018-25190

http://www.cnvd.org.cn/flaw/show/CNVD-2018-25192

http://www.cnvd.org.cn/flaw/show/CNVD-2018-25193

http://www.cnvd.org.cn/flaw/show/CNVD-2018-25194

http://www.cnvd.org.cn/flaw/show/CNVD-2018-25195

http://www.cnvd.org.cn/flaw/show/CNVD-2018-25196

http://www.cnvd.org.cn/flaw/show/CNVD-2018-25197

2、IBM 产品安全漏洞

IBM QRadar Advisor with Watson 是一套安全威胁分析解决方案。IBM QRadar Incident Forensics 是一套安全取证调查软件。IBM DataPower Gateway 是一套专门为移动、云、应用编程接口（API）、网络、面向服务架构（SOA）、B2B 和云工作负载而设

计的安全和集成平台，它可利用专用网关平台跨渠道保护、集成和优化访问。IBM SDK 是一套用于创建、发现、调用和测试 Web 服务的集成工具包。IBM Campaign（前称 Unica Campaign）是一套用于帮助营销人员设计、执行、衡量和优化营销广告的管理解决方案。IBM Security Access Manager 是一款应用于信息安全管理的产品。IBM BigFix Platform 是一套动态的集成了消息内容驱动和管理系统的多技术平台。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，提升权限，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：IBM QRadar Advisor with Watson 信息泄露漏洞、IBM QRadar Incident Forensics 信息泄露漏洞（CNVD-2018-25037）、IBM DataPower Gateway 拒绝服务漏洞、IBM SDK java.math 组件拒绝服务漏洞、IBM Campaign 权限访问控制漏洞、IBM Security Access Manager 信息泄露漏洞（CNVD-2018-25399、CNVD-2018-25404）、IBM BigFix Platform 信息泄露漏洞（CNVD-2018-25405）。其中，“IBM Campaign 权限访问控制漏洞”的综合评级为为“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-2018-25036
http://www.cnvd.org.cn/flaw/show/CNVD-2018-25037
http://www.cnvd.org.cn/flaw/show/CNVD-2018-25183
http://www.cnvd.org.cn/flaw/show/CNVD-2018-25304
http://www.cnvd.org.cn/flaw/show/CNVD-2018-25312
http://www.cnvd.org.cn/flaw/show/CNVD-2018-25399
http://www.cnvd.org.cn/flaw/show/CNVD-2018-25404
http://www.cnvd.org.cn/flaw/show/CNVD-2018-25405

3、Siemens 产品安全漏洞

Siemens SINUMERIK 808D 等都是数控机床系统控制器。Siemens TIM 1531 IRC 是一款通信模块。Siemens EN100 Ethernet Communication Module 是一款以太网模块产品。SIPROTEC 5 relays 是一款继电器。Siemens SIMATIC S7-400 是一款用于制造和过程自动化领域的可编程逻辑控制器产品。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞进行越界读取，任意写入，执行代码，造成拒绝服务，影响系统的保密性、可用性和完整性。

CNVD 收录的相关漏洞包括：多款 Siemens 产品整数溢出漏洞、多款 Siemens 产品缓冲区溢出漏洞、多款 Siemens 产品本地访问权限漏洞、多款 Siemens 产品远程代码执行漏洞、Siemens TIM 1531 IRC 身份验证漏洞、Siemens EN100 Ethernet Communication Module 和 SIPROTEC 5 relays 拒绝服务漏洞、Siemens EN100 Ethernet Communication Module 拒绝服务漏洞、Siemens SIMATIC S7-400 输入验证漏洞。上述漏洞的综

合评级为为“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-2018-25415

http://www.cnvd.org.cn/flaw/show/CNVD-2018-25420

http://www.cnvd.org.cn/flaw/show/CNVD-2018-25422

http://www.cnvd.org.cn/flaw/show/CNVD-2018-25423

http://www.cnvd.org.cn/flaw/show/CNVD-2018-25424

http://www.cnvd.org.cn/flaw/show/CNVD-2018-25425

http://www.cnvd.org.cn/flaw/show/CNVD-2018-25426

http://www.cnvd.org.cn/flaw/show/CNVD-2018-25433

4、Google 产品安全漏洞

Google Chrome 是一款 Web 浏览器。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。Google Kubernetes 是一套开源的 Docker 容器集群管理系统。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，绕过权限策略，执行任意代码。

CNVD 收录的相关漏洞包括：Google Chrome 权限绕过漏洞、Google Android 缓冲区溢出漏洞（CNVD-2018-25279）、Google Chrome DevTools 代码执行漏洞、Google Chrome Skia 任意代码执行漏洞、Google Chrome Service Worker 信息泄露漏洞、Google Chrome WebAssembly 内存错误引用漏洞、Google Kubernetes 权限访问控制漏洞、Google Chrome PDFium 内存错误引用漏洞（CNVD-2018-25308）。其中，除“Google Chrome Service Worker 信息泄露漏洞”外，其余漏洞的综合评级为为“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-2018-25277

http://www.cnvd.org.cn/flaw/show/CNVD-2018-25279

http://www.cnvd.org.cn/flaw/show/CNVD-2018-25280

http://www.cnvd.org.cn/flaw/show/CNVD-2018-25283

http://www.cnvd.org.cn/flaw/show/CNVD-2018-25305

http://www.cnvd.org.cn/flaw/show/CNVD-2018-25307

http://www.cnvd.org.cn/flaw/show/CNVD-2018-25306

http://www.cnvd.org.cn/flaw/show/CNVD-2018-25308

5、Anker Nebula Capsule Pro 拒绝服务漏洞

Anker Nebula Capsule Pro 是一款投影仪设备。本周，Anker Nebula Capsule Pro 被披露存在拒绝服务漏洞。攻击者可借助特制的应用程序向 WifiService 发送数据利用该漏洞造成拒绝服务（底层 Android 7.1.2 操作系统重启）。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-201

8-25278

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-2018-24942	ThinkPHP5 远程代码执行漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://blog.thinkphp.cn/869075
CNVD-2018-25029	MiniShare 缓冲区溢出漏洞	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://minishare.sourceforge.net/
CNVD-2018-25041	Pluck 跨站请求伪造漏洞	高	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法：https://www.pluck-cms.org/
CNVD-2018-25054	Summit 远程代码执行漏洞	高	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法：https://npmjs.org/package/summit
CNVD-2018-25169	Adobe Acrobat 和 Reader 存在堆栈溢出漏洞	高	Adobe 已经为此发布了一个安全公告（APSB18-09）以及相应补丁：https://helpx.adobe.com/security/products/acrobat/apsb18-09.html
CNVD-2018-25180	ASUSTOR ADM 操作系统命令注入漏洞	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：https://www.asustor.com/
CNVD-2018-25184	Linux kernel 内存泄露漏洞（CNVD-2018-25184）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.19.3
CNVD-2018-25187	FreeBSD 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://security.freebsd.org/advisories/FreeBSD-SA-18:14.bhyve.asc
CNVD-2018-25276	Microsoft Edge 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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8464
CNVD-201	多款 RICOH Interactive White	高	厂商已发布了漏洞修复程序，请及时

8-25435	board 产品 SQL 注入漏洞		关注更新：https://www.ricoh.com/info/2018/1127_1.html

小结：本周，Foxit 被披露存在内存错误引用漏洞，攻击者可利用漏洞在当前进程的上下文中执行代码。此外，IBM、Siemens、Google 等多款产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，绕过权限策略，提升权限，执行任意代码，发起拒绝服务攻击等。另外，Anker Nebula Capsule Pro 被披露存在拒绝服务漏洞。攻击者可借助特制的应用程序向 WifiService 发送数据利用该漏洞造成拒绝服务（底层 Android 7.1.2 操作系统重启）。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。

本周重要漏洞攻击验证情况

本周，CNVD 建议注意防范以下已公开漏洞攻击验证情况。

1、Tarantella Enterprise 路径遍历漏洞

验证描述

Tarantella Enterprise 是一个数据和应用程序集中管理工具，提供 Web 管理接口，可以运行于大多数 Unix 和 Linux 平台。

Tarantella Enterprise 3.11 之前版本中存在路径遍历漏洞。攻击者可利用该漏洞访问存储在文件系统上的任意文件和目录。

验证信息

POC 链接：https://packetstormsecurity.com/files/150541/Tarantella-Enterprise-Directory-Traversal.html

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2018-25284

信息提供者

恒安嘉新(北京)科技股份公司

注：以上验证信息(方法)可能带有攻击性，仅供安全研究之用。请广大用户加强对漏洞的防范工作，尽快下载相关补丁。

本周漏洞要闻速递

1. Google Play 里的 22 款应用发现含有后门

Sophos 公司的安全研究人员从 Google Play 官方应用商店发现了 22 款包含后门的应用，应用的总下载量超过 200 万，最流行的一款是手电筒应用 Sparkle Flashlight，其下载量超过一百万。应用含有的后门能悄悄从攻击者控制的服务器上下载文件。这些应用主要被用于广告欺诈，研究人员将它们命名为 Andr/Clickr-ad，通过欺骗性的广告点

击获取收入，它给用户带来的问题是电池续航力的下降和数据流量的增加。后门潜在可用于下载任何恶意程序。Google 已经从商店里移除了这些恶意应用。

参考链接：https://www.solidot.org/story?sid=58869

2. Mint 木马变种泛滥，伪装“抖音电脑版”肆虐网络

近期，某安全实验室发现一款名为“西瓜看图”的恶意软件。该软件主要通过“荒野行动电脑版”、“抖音电脑版”等虚假下载器进行传播。该虚假器运行后，实际安装的是“蜻蜓助手”安卓模拟器，并由“蜻蜓助手”推广安装“西瓜看图”木马远控软件。该软件通过云控手段，进行主页劫持、图标推广、软件推广、广告弹窗等恶意行为。由于该木马会在用户磁盘中创建“Mint”的目录，保存云控插件，所以我们特此命名为“Mint”木马。

参考链接：https://www.freebuf.com/news/191461.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：010-82991537