国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2018 年 7 月 16 日-2018 年 7 月 22 日 **2018 年第 29 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 257 个，其中高危漏洞 58 个、中危漏洞 194 个、低危漏洞 5 个。漏洞平均分值为 5.70。本周收录的漏洞中，涉及 0day 漏洞 66 个（占 27%），其中互联网上出现“Modx Revolution 远程代码执行漏洞、Intex N150 设备跨站请求伪造漏洞”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 566 个，与上周（456 个）环比增长 24%。

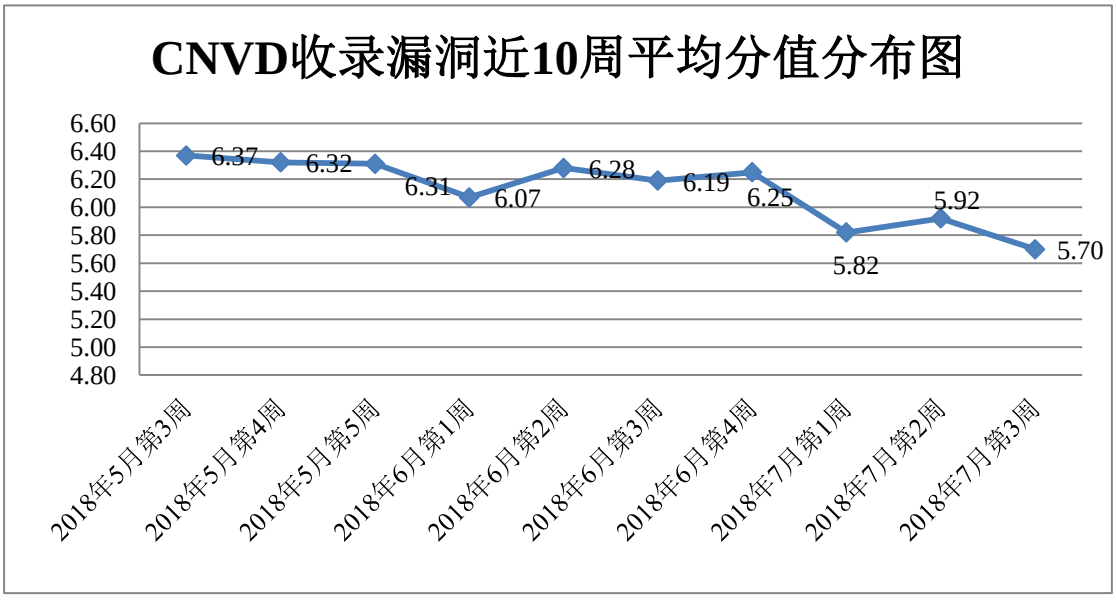

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，阿里云计算有限公司、北京天融信网络安全技术有限公司、北京启明星辰信息安全技术有限公司、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、中新网络信息安全股份有限公司、上海银基信息安全技术股份有限公司、四川博全科技有限公司、上海谋乐网络科技有限公司、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、海南神州希望网络有限公司、山石网科通信技术有限公司、安徽锋刃信息科技有限公司、南京联成科技发展股份有限公司、广州竞远安全技术股份有限公司、广州万方计算机科技有限公司、四川虹微技术有限公司（子午攻防实验室）、南昌远图科技有限公司、北京明朝万达科技股份有限公司（安元实验室）及其他个人白帽子向 CNVD 提交了 566 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 295 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
阿里云计算有限公司	707	0
北京天融信网络安全技术有限公司	421	13
北京启明星辰信息安全技术有限公司	274	0
哈尔滨安天科技股份有限公司	224	0
漏洞盒子	217	217
华为技术有限公司	177	0
北京数字观星科技有限公司	117	0
新华三技术有限公司	105	0
北京神州绿盟科技有限公司	98	0
中国电信集团系统集成有限责任公司	98	0
360 网神（补天平台）	78	78
杭州安恒信息技术有限公司	76	0
恒安嘉新(北京)科技股份公司	57	0
深圳市深信服电子科技有限公司	39	0
北京无声信息技术有限公司	19	0

厦门服云信息科技有限公司	7	0
北京知道创宇信息技术有限公司	3	0
山东云天安全技术有限公司	77	77
中新网络信息安全股份有限公司	12	12
上海银基信息安全技术股份有限公司	10	10
四川博全科技有限公司	6	6
上海谋乐网络科技有限公司	5	5
河南信安世纪科技有限公司	5	5
任子行网络技术股份有限公司	4	4
海南神州希望网络有限公司	3	3
山石网科通信技术有限公司	3	3
安徽锋刃信息科技有限公司	2	2
南京联成科技发展股份有限公司	2	2
广州竞远安全技术股份有限公司	1	1
广州万方计算机科技有限公司	1	1
四川虹微技术有限公司（子午攻防实验室）	1	1
南昌远图科技有限公司	1	1
北京明朝万达科技股份有限公司（安元实验室）	1	1
CNCERT 贵州分中心	5	5
CNCERT 新疆分中心	5	5
CNCERT 湖南分中心	2	2
CNCERT 吉林分中心	2	2

CNCERT 宁夏分中心	2	2
个人	108	108
报送总计	2975	566

本周漏洞按类型和厂商统计

本周，CNVD 收录了 257 个漏洞。其中应用程序漏洞 185 个，WEB 应用漏洞 37 个，操作系统漏洞 17 个，网络设备漏洞 10 个，安全产品漏洞 4 个，数据库漏洞 4 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	185
WEB 应用漏洞	37
操作系统漏洞	17
网络设备漏洞	10
安全产品漏洞	4
数据库漏洞	4

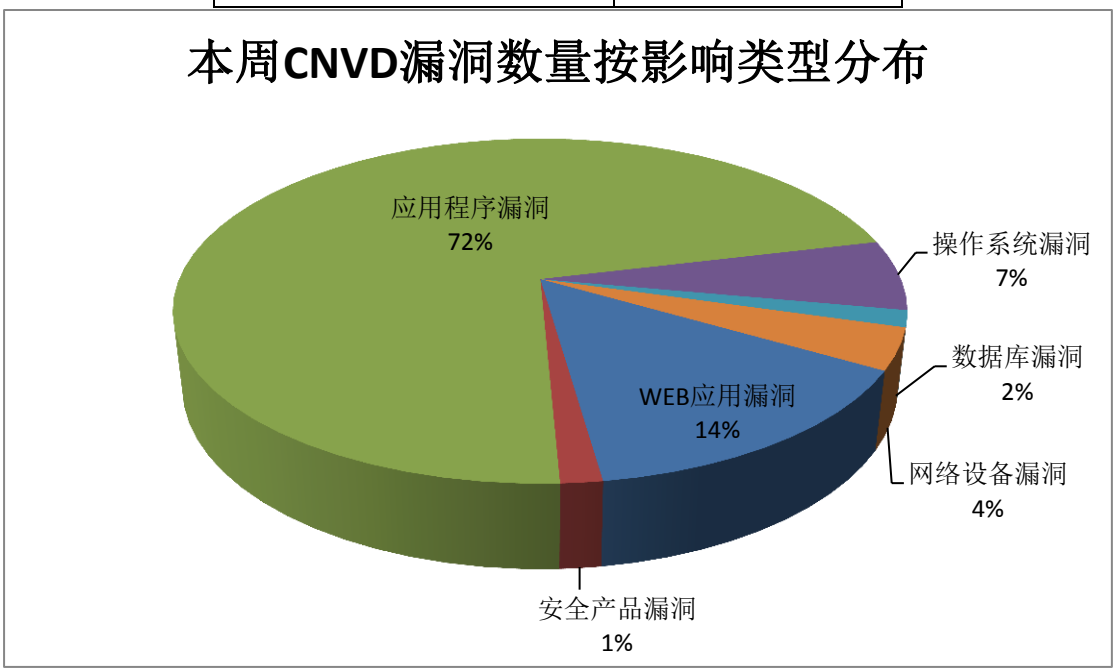

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、Microsoft、Oracle 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	Adobe	50	19%

2	Microsoft	26	10%
3	Oracle	17	7%
4	IBM	8	3%
5	Dolibarr	4	2%
6	Jirafeau	4	2%
7	OneFileCMS	4	2%
8	Palo Alto Networks	4	2%
9	Bootstrap	3	1%
10	其他	137	52%

本周行业漏洞收录情况

本周，CNVD 收录了 10 个电信行业漏洞，4 个移动互联网行业漏洞，5 个工控行业漏洞（如下图所示）。其中，“Oracle WebLogic 反序列化远程代码执行漏洞、IBM DB2 提权漏洞 、Oracle Fusion Middleware Oracle WebLogic Server 组件远程漏洞（CNVD-2018-13562）”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/

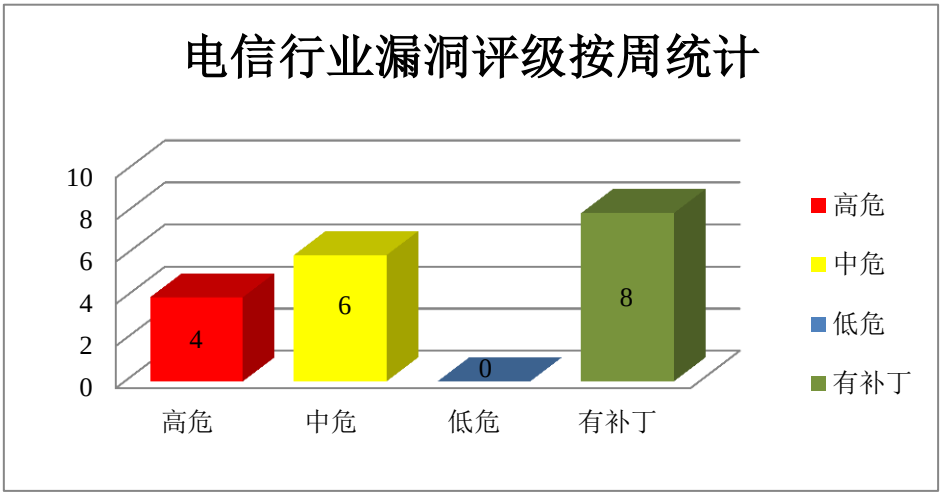

图 3 电信行业漏洞统计

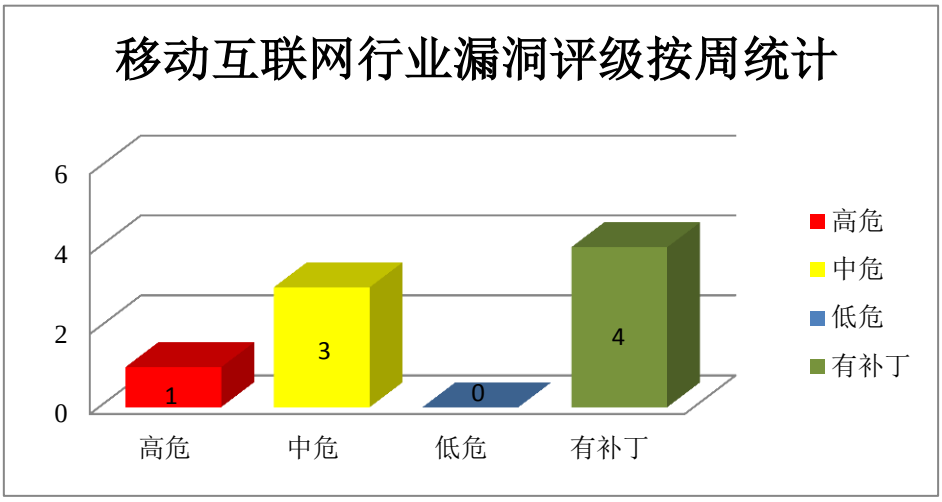

图 4 移动互联网行业漏洞统计

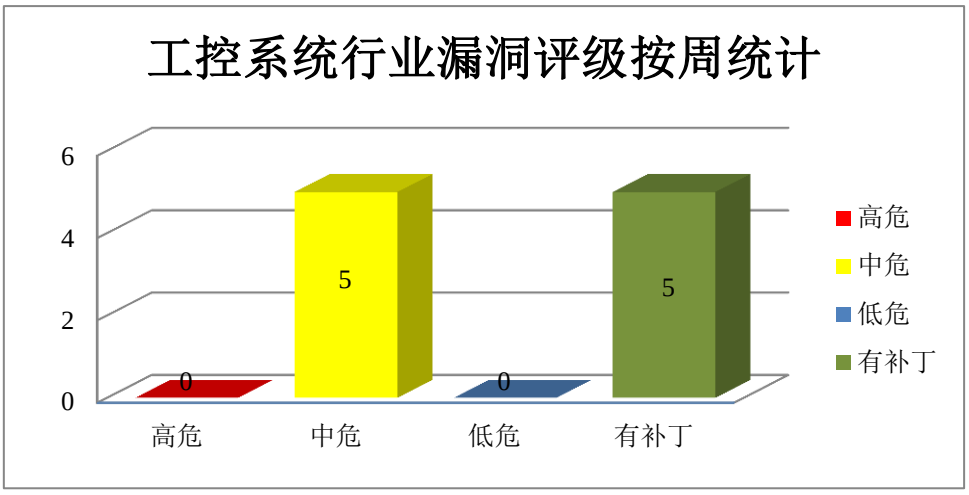

图 5 工控系统行业漏洞统计

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、Adobe 产品安全漏洞

Adobe Acrobat 是一款 PDF 编辑软件。Adobe Reader(也被称为 Acrobat Reader)是一款 PDF 文件阅读软件。本周，上述产品被披露存在类型混淆和缓冲区溢出漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Flash Player 类型混淆漏洞（CNVD-2018-13400）、Adobe Acrobat 和 Reader 缓冲区溢出漏洞（CNVD-2018-13402、CNVD-2018-13401、CNVD-2018-13404、CNVD-2018-13403）、Adobe Acrobat 和 Reader 类型混淆漏洞（CNVD-2018-13406、CNVD-2018-13405、CNVD-2018-13407）。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-2018-13400

http://www.cnvd.org.cn/flaw/show/CNVD-2018-13402

http://www.cnvd.org.cn/flaw/show/CNVD-2018-13401

http://www.cnvd.org.cn/flaw/show/CNVD-2018-13404

http://www.cnvd.org.cn/flaw/show/CNVD-2018-13403

http://www.cnvd.org.cn/flaw/show/CNVD-2018-13406

http://www.cnvd.org.cn/flaw/show/CNVD-2018-13405

http://www.cnvd.org.cn/flaw/show/CNVD-2018-13407

2、Microsoft 产品安全漏洞

Microsoft Wireless Display Adapter V2 Software 是一套用于支持显示设备投影的软件。Microsoft Windows 7 是一套个人电脑使用的操作系统。Windows Server 2012 R2 是一套服务器操作系统。Microsoft SharePoint 是一套企业业务协作平台。Microsoft SharePoint Enterprise Server 2016 是一套企业业务协作平台。SharePoint Foundation 2013 SP1 是一套基于 Web 的面向小型组织或部门的协作平台。Microsoft Office 是一款办公软件套件产品。Microsoft ChakraCore 是一个 Edge（Web 浏览器）所使用的 JavaScript 引擎的核心部分。本周，上述产品被披露存在多个漏洞，攻击者可利用提升权限，执行任意代码，破坏内存。

CNVD 收录的相关漏洞包括：Microsoft Chakra 脚本引擎远程内存破坏漏洞、Microsoft Windows 权限提升漏洞（CNVD-2018-13360）、Microsoft SharePoint 远程代码执行漏洞（CNVD-2018-13361）、Microsoft Wireless Display Adapter 命令注入漏洞、Microsoft Windows 权限提升漏洞（CNVD-2018-13363）、Microsoft SharePoint 权限提升漏洞（CNVD-2018-13383、CNVD-2018-13385）、Microsoft Office 远程代码执行漏洞（CNVD-2018-13382）。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-2018-13333

http://www.cnvd.org.cn/flaw/show/CNVD-2018-13360

http://www.cnvd.org.cn/flaw/show/CNVD-2018-13361

http://www.cnvd.org.cn/flaw/show/CNVD-2018-13359

http://www.cnvd.org.cn/flaw/show/CNVD-2018-13363

http://www.cnvd.org.cn/flaw/show/CNVD-2018-13383

http://www.cnvd.org.cn/flaw/show/CNVD-2018-13385

http://www.cnvd.org.cn/flaw/show/CNVD-2018-13382

3、Oracle 产品安全漏洞

WebLogic 是一个 application server，是一个基于 JAVAEE 架构的中间件，WebLogic 是用于开发、集成、部署和管理大型分布式 Web 应用、网络应用和数据库应用的 Jav

a 应用服务器。Oracle Fusion Middleware（Oracle 融合中间件）是一套面向企业和云环境的业务创新平台。Java SE（Java 平台标准版）用于开发和部署桌面、服务器以及嵌入设备和实时环境中的 Java 应用程序；Java SE Embedded 是一款针对嵌入式系统开发功能强大、可靠、可移植的应用程序的 Java 平台。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞影响机密性、完整性及可用性。

CNVD 收录的相关漏洞包括：Oracle WebLogic 反序列化远程代码执行漏洞、Oracle Fusion Middleware Oracle WebLogic Server 组件远程漏洞（CNVD-2018-13562、CNVD-2018-13563、CNVD-2018-13567、CNVD-2018-13568）、Oracle Java SE 和 Java SE Embedded 远程漏洞、Oracle Java SE 存在未明漏洞（CNVD-2018-13569、CNVD-2018-13570）。其中，“Oracle WebLogic 反序列化远程代码执行漏洞、Oracle Fusion Middleware Oracle WebLogic Server 组件远程漏洞（CNVD-2018-13562）、Oracle Java SE 存在未明漏洞（CNVD-2018-13569、CNVD-2018-13570）”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-2018-13334
http://www.cnvd.org.cn/flaw/show/CNVD-2018-13562
http://www.cnvd.org.cn/flaw/show/CNVD-2018-13563
http://www.cnvd.org.cn/flaw/show/CNVD-2018-13566
http://www.cnvd.org.cn/flaw/show/CNVD-2018-13567
http://www.cnvd.org.cn/flaw/show/CNVD-2018-13568
http://www.cnvd.org.cn/flaw/show/CNVD-2018-13569
http://www.cnvd.org.cn/flaw/show/CNVD-2018-13570

4、IBM 产品安全漏洞

IBM FileNet Content Manager 是一套针对 FileNet P8 平台的内容管理解决方案。IBM Planning Analytics 是一套业务规划分析解决方案。IBM DB2 是一套关系型数据库管理系统。IBM WebSphere Application Server（WAS）是一款应用服务器产品，它是 Java EE 和 Web 服务应用程序的平台，也是 IBM WebSphere 软件平台的基础。Liberty 是 WAS 的一个动态服务器配置文件。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，劫持用户会话，提升权限。

CNVD 收录的相关漏洞包括：IBM FileNet Content Manager 跨站脚本漏洞（CNVD-2018-13367、CNVD-2018-13447）、IBM Planning Analytics 跨站脚本漏洞、IBM DB2 提权漏洞（CNVD-2018-13456、CNVD-2018-13457、CNVD-2018-13458）、IBM WebSphere Application Server 信息泄露漏洞（CNVD-2018-13466）、IBM WebSphere Application Server Liberty 信息泄露漏洞（CNVD-2018-13472）。其中，“IBM DB2 提权漏洞（CNVD-2018-13456、CNVD-2018-13458）”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-2018-13367
http://www.cnvd.org.cn/flaw/show/CNVD-2018-13447
http://www.cnvd.org.cn/flaw/show/CNVD-2018-13455
http://www.cnvd.org.cn/flaw/show/CNVD-2018-13456
http://www.cnvd.org.cn/flaw/show/CNVD-2018-13457
http://www.cnvd.org.cn/flaw/show/CNVD-2018-13458
http://www.cnvd.org.cn/flaw/show/CNVD-2018-13466
http://www.cnvd.org.cn/flaw/show/CNVD-2018-13472

5、Cisco Unified Computing System 本地命令注入漏洞（CNVD-2018-13560）

Cisco Unified Computing System（UCS）Software 是美国思科（Cisco）公司的一套统一计算系统。该系统通过大量采用虚拟化技术将网络、计算和虚拟化资源集成到一个平台上。本周，Cisco UCS Software 被披露存在本地命令注入漏洞，该漏洞源于程序对文件系统缺少验证和输入检测。本地攻击者可通过在受影响系统的 CLI 中发布特制的命令利用该漏洞在受影响系统上执行任意命令。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-2018-13560

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-2018-13557	Dell EMC iDRAC 不安全文件权限漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://www.dell.com/support/article/cn/zh/cnbsd1/sln310281/ism-dell-emc-idrac-service-module-improper-file-permission-vulnerability?lang=en
CNVD-2018-13200	Fortify Software Security Center (SSC) XXE 漏洞	高	用户可联系供应商获得补丁信息：https://www.microfocus.com
CNVD-2018-13199	Zeta Producer Desktop CMS 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.zeta-producer.com/de/download.html
CNVD-2018-13240	ManageEngine Exchange Reporter Plus 远程代码执行漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://www.manageengine.com/products/exchange-reports/release-notes.html
CNVD-201	Haxx curl 'Curl_smtp_escape_	高	厂商已发布漏洞修复程序，请及时关

8-13252	eob'函数堆缓冲区溢出漏洞		注更新：https://github.com/curl/curl/commit/ba1dbd78e5f1ed67c1b8d37ac89d90e5e330b628
CNVD-2018-13286	Microsoft Publisher 权限提升漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8245
CNVD-2018-13345	reSIProcate 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://github.com/resiprocate/resiprocate/commit/2cb291191c93c7c4e371e22cb89805a5b31d6608
CNVD-2018-13357	OCS Inventory NG SQL 注入漏洞（CNVD-2018-13357）	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.ocsinventory-ng.org/en/ocs-inventory-server-2-4-1-has-been-released/
CNVD-2018-13460	Dolibarr ERP/CRM SQL 注入漏洞（CNVD-2018-13460）	高	厂商已发布漏洞修复程序，请及时关注更新：https://github.com/Dolibarr/dolibarr/commit/36402c22eef49d60edd73a2f312f8e28fe0bd1cb
CNVD-2018-13476	Cisco Policy Suite Cluster Manager 默认密码漏洞	高	用户可联系供应商获得补丁信息：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180718-policy-cm-default-psswrd

小结：本周，Adobe 被披露存在类型混淆和缓冲区溢出漏洞，攻击者可利用漏洞执行任意代码。此外，Microsoft、Oracle、IBM 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，劫持用户会话，提升权限，执行任意代码，破坏内存等。另外，Cisco Unified Computing System 存在本地命令注入漏洞，本地攻击者可通过在受影响系统的 CLI 中发布特制的命令利用该漏洞在受影响系统上执行任意命令。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. 国产扫地机器人缔奇 360 被曝存在安全漏洞，秒变监视器

近日，两位安全研究员公布了影响到缔奇（Diqee）360 扫地机器人的两个漏洞的相关信息。这两个漏洞分别是 CVE-2018-10987 和 CVE-2018-10988。第一个可以通过远程利用，而第二个需要对设备的物理访问。允许攻击者在具有超级用户特权的设备上运行

恶意代码，并有效地对其进行接管。

参考链接：https://www.easyaq.com/news/1075137218.shtml

2. Apache Struts2 高危漏洞致企业服务器被入侵安装 KoiMiner 挖矿木马

许多企业的网站使用 Apache 的开源项目搭建 http 服务器，其中又有很大部分使用了 Apache 子项目 Struts。但由于 Apache Struts2 产品代码存在较多隐患，从 2007 年开始 Struts2 就频频爆出多个高危漏洞。近期，再次监测到类似的攻击。黑客利用攻击工具 WinStr045 检测网络上存在漏洞的 web 服务器，发现存在漏洞的机器后通过远程执行各类指令进行提权、创建账户、系统信息搜集，然后将用于下载的木马 mas.exe 植入，进而利用 mas.exe 这个木马下载器从多个 C&C 地址下载更多木马：利用提权木马 o3/o6.exe、挖矿木马 netxmr4.0.exe。

参考链接：http://www.freebuf.com/vuls/176847.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