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 23 日-2018 年 7 月 29 日 **2018 年第 30 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 214 个，其中高危漏洞 50 个、中危漏洞 158 个、低危漏洞 6 个。漏洞平均分值为 5.84。本周收录的漏洞中，涉及 0day 漏洞 66 个（占 31%），其中互联网上出现“ZOHO ManageEngine ServiceDesk Plus 用户权举漏洞、EMS Master Calendar 跨站脚本漏洞”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 807 个，与上周（566 个）环比增长 42%。

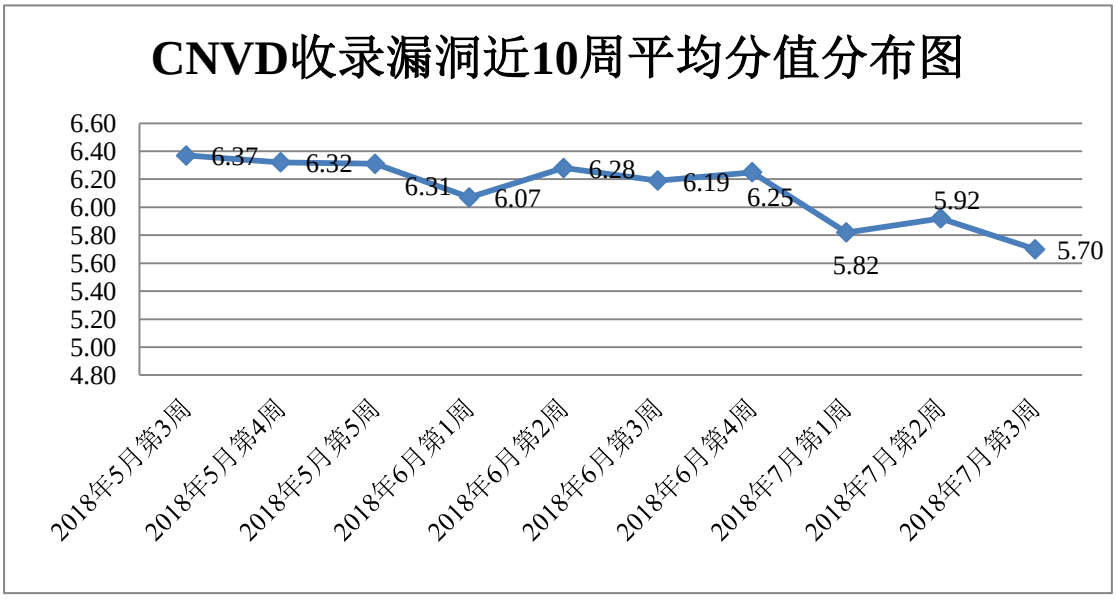

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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、中国电信集团系统集成有限责任公司、新华三

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、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、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、河北盾安科技有限公司、新疆海狼科技有限公司、北京智游网安科技有限公司、山石网科通信技术有限公司、江苏君立华域信息安全技术有限公司、河北网信智安信息技术有限公司、上海银基信息安全技术股份有限公司、广州万方计算机科技有限公司、北京国舜科技股份有限公司、北京明朝万达科技股份有限公司（安元实验室）、安徽锋刃信息科技有限公司、国家互联网应急中心研究所，北京同余科技有限公司及其他个人白帽子向 CNVD 提交了 807 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 481 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	348	13
漏洞盒子	278	278
哈尔滨安天科技股份有限公司	216	0
360 网神（补天平台）	203	203
华为技术有限公司	132	0
中国电信集团系统集成有限责任公司	81	0
新华三技术有限公司	75	0
北京数字观星科技有限公司	68	0
北京神州绿盟科技有限公司	54	0
恒安嘉新(北京)科技股份公司	50	0
北京无声信息技术有限公司	11	0
北京知道创宇信息技术有限公司	7	2
深圳市深信服电子科技有限公司	6	0
北京启明星辰信息安全技术有限公司	5	5

厦门服云信息科技有限公司	3	0
杭州安恒信息技术有限公司	2	0
山东云天安全技术有限公司	80	80
南京联成科技发展股份有限公司	14	14
中新网络信息安全股份有限公司	10	10
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
河北盾安科技有限公司	2	2
新疆海狼科技有限公司	2	2
北京智游网安科技有限公司	2	2
山石网科通信技术有限公司	1	1
江苏君立华域信息安全技术有限公司	1	1
河北网信智安信息技术有限公司	1	1
上海银基信息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
北京国舜科技股份有限公司	1	1
北京明朝万达科技股份有限公司（安元实验室）	1	1
安徽锋刃信息科技有限公司	1	1
国家互联网应急中心研究所，北京同余科技有限公司	1	1
CNCERT 上海分中心	23	23
CNCERT 山西分中心	17	17

CNCERT 新疆分中心	9	9
CNCERT 吉林分中心	9	9
CNCERT 湖南分中心	8	8
CNCERT 海南分中心	5	5
CNCERT 陕西分中心	4	4
CNCERT 天津分中心	4	4
CNCERT 宁夏分中心	2	2
CNCERT 甘肃分中心	2	2
CNCERT 广东分中心	1	1
CNCERT 贵州分中心	1	1
个人	93	93
报送总计	1845	807

本周漏洞按类型和厂商统计

本周，CNVD 收录了 214 个漏洞。其中应用程序漏洞 144 个，WEB 应用漏洞 41 个，网络设备漏洞 27 个，操作系统漏洞 1 个，数据库漏洞 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	144
WEB 应用漏洞	41
网络设备漏洞	27
操作系统漏洞	1
数据库漏洞	1

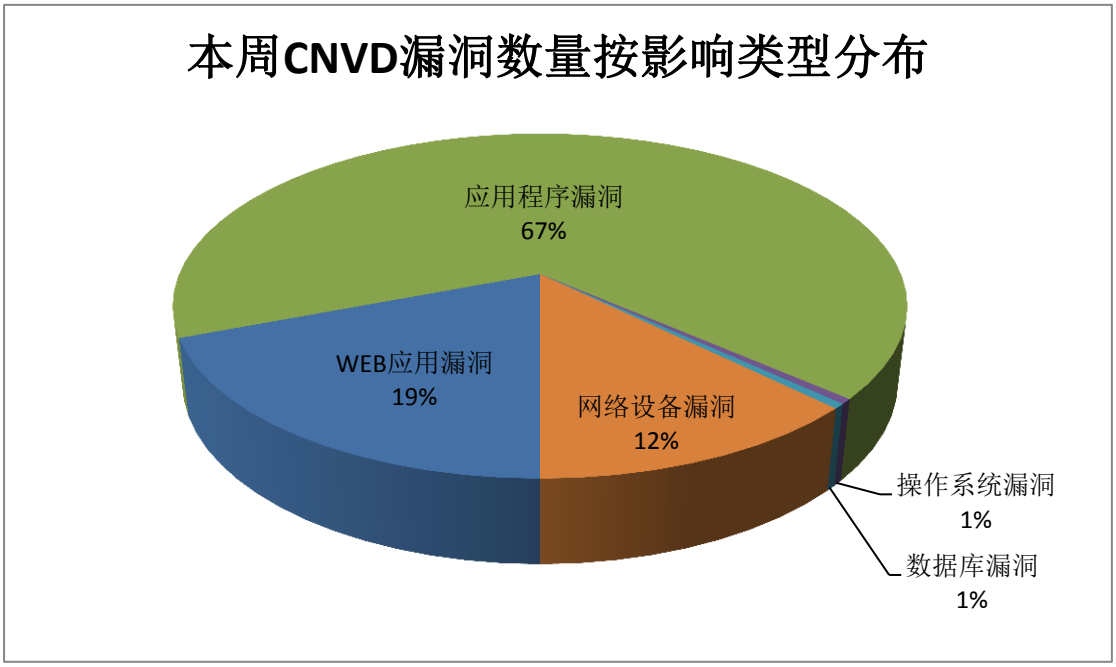

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Cisco、Foxit、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	Cisco	16	8%
2	Foxit	15	7%
3	IBM	13	6%
4	Mozilla	10	5%
5	WordPress	9	4%
6	npm	7	3%
7	Oracle	7	3%
8	Wireshark	7	3%
9	Intel	6	3%
10	其他	124	58%

本周行业漏洞收录情况

本周，CNVD 收录了 22 个电信行业漏洞，4 个移动互联网行业漏洞，4 个工控行业漏洞（如下图所示）。其中，“多款 Advantech 产品堆缓冲区溢出漏洞、Cisco Nexus 9000 Series Fabric Switches DHCPv6 功能拒绝服务漏洞、多款 Advantech 产品权限提升

漏洞、Cisco SD-WAN Solution 远程文件覆盖漏洞、Polaris Office 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/

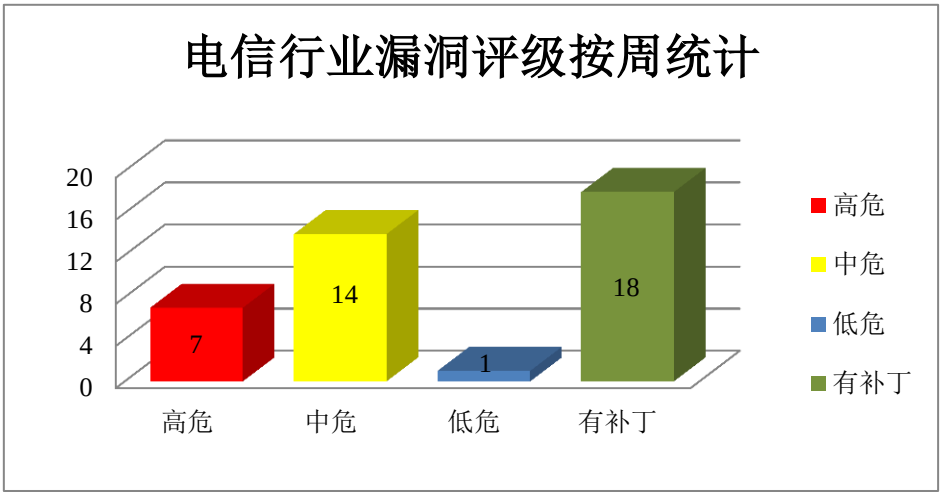

图 3 电信行业漏洞统计

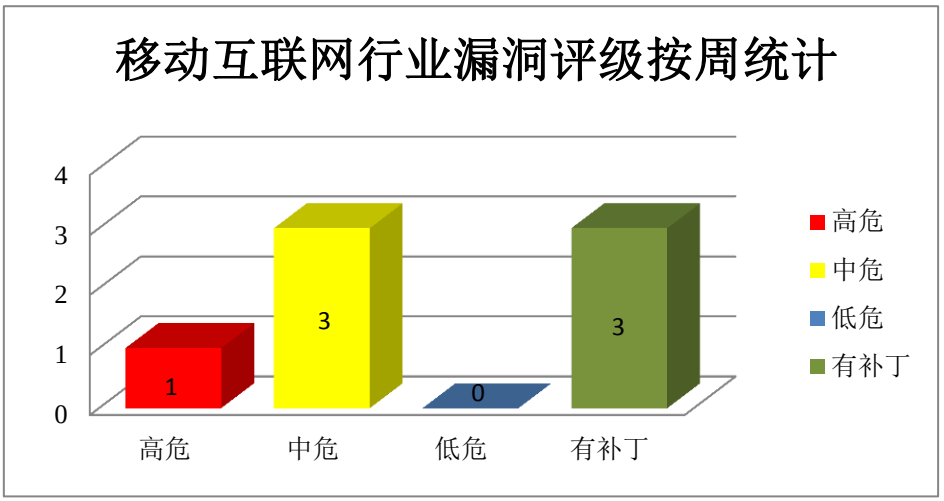

图 4 移动互联网行业漏洞统计

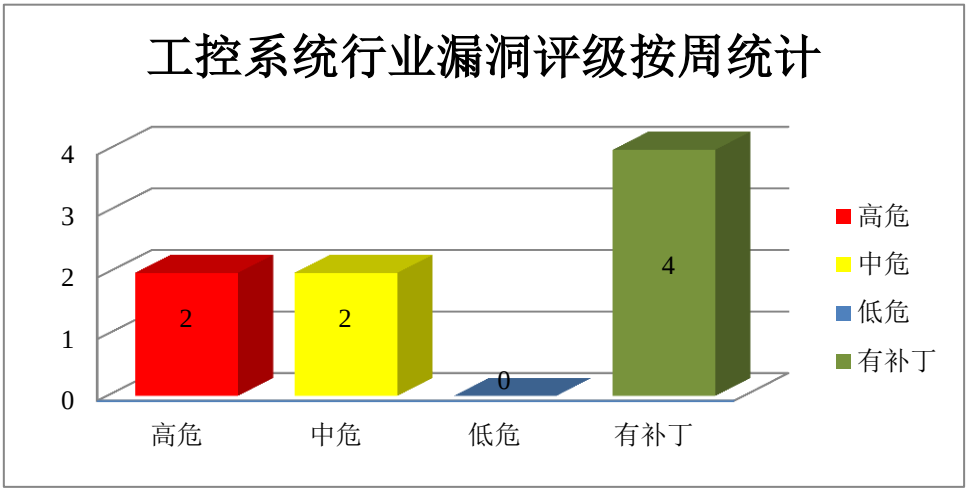

图 5 工控系统行业漏洞统计

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、Cisco 产品安全漏洞

Cisco vBond Orchestrator Software 和 vManage Network Management Software 都是网络管理软件。Smart Controller Software 是一套智能网络控制软件。SD-WAN Solution 是运行在其中的一套网络扩展解决方案。vEdge 100 Series Routers 是一款 100 系列的路由器产品。Cisco Nexus 9000 Series Fabric Switches 是一款 9000 系列交换机产品。Cisco Webex Teams 是一款团队协作应用程序。该程序包括视频会议、消息群发和文件共享等功能。本周，上述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或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco SD-WAN Configuration and Management Database 远程代码执行漏洞、Cisco SD-WAN Solution 远程命令注入漏洞（CNVD-2018-14074、CNVD-2018-14079、CNVD-2018-14083）、Cisco SD-WAN Solution 远程文件覆盖漏洞、Cisco SD-WAN Zero Touch Provisioning 拒绝服务漏洞、Cisco Nexus 9000 Series Fabric Switches DHCPv6 功能拒绝服务漏洞、Cisco Webex Teams 远程代码执行漏洞。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-2018-14073

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14074

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14076

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14079

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14078

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14080

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14081

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14083

2、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。本周，上述产品被披露存在内存错误引用、缓冲区溢出和远程代码执行漏洞，攻击者可利用执行任意代码。

CNVD 收录的相关漏洞包括：Foxit Reader 缓冲区溢出漏洞（CNVD-2018-13985）、Foxit Reader ExpaseFDF 任意文件编写远程代码执行漏洞、Foxit Reader 内存错误引用漏洞（CNVD-2018-14146、CNVD-2018-14147、CNVD-2018-14148、CNVD-2018-14149、CNVD-2018-14150、CNVD-2018-14151）。其中，“Foxit Reader 缓冲区溢出漏洞（CNVD-2018-13985）、Foxit Reader ExpaseFDF 任意文件编写远程代码执行漏洞”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-2018-13985

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14066

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14146

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14147

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14148

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14149

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14150

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14151

3、IBM 产品安全漏洞

IBM InfoSphere Data Replication Dashboard 是一套数据同步解决方案。IBM Sterling B2B Integrator 是一套集成了重要的 B2B 流程、交易和关系的软件。IBM Sterling File Gateway 是的一套文件传输软件。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，读取任意文件，注入任意的 Web 脚本或 HTML。

CNVD 收录的相关漏洞包括：IBM InfoSphere Data Replication Dashboard 跨站脚本漏洞、IBM InfoSphere Data Replication Dashboard 路径遍历漏洞、IBM InfoSphere Data Replication Dashboard SQL 注入漏洞、IBM Sterling B2B Integrator 信息泄露漏洞（CNVD-2018-14084、CNVD-2018-14085）、IBM Sterling File Gateway 信息泄露漏洞（CNVD-2018-14087、CNVD-2018-14088、CNVD-2018-14094）。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-2018-13683

http://www.cnvd.org.cn/flaw/show/CNVD-2018-13685

http://www.cnvd.org.cn/flaw/show/CNVD-2018-13684

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14084

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14087

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14085

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14088

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14094

4、Mozilla 产品安全漏洞

Mozilla Firefox 是一款开源 Web 浏览器；Firefox ESR 是 Firefox 的一个延长支持版本。Skia 是其中的一个开放源码的 2D 图形库，能够提供可在各种硬件和软件平台上工作的常见 API。Mozilla Thunderbird 是、从 Mozilla Application Suite 独立出来的电子邮件客户端软件，支持 IMAP、POP 邮件协议以及 HTML 邮件格式。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，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：Mozilla Thunderbird 信息泄露漏洞（CNVD-2018-13663、CNVD-2018-13662、CNVD-2018-14109）、Mozilla Firefox 代码执行漏洞（CNVD-2018-13863、CNVD-2018-13891）、Mozilla Firefox 整数溢出漏洞（CNVD-2018-13885）、Mozilla Firefox 越权漏洞、Mozilla Firefox 信息泄露漏洞（CNVD-2018-13964）。其中，“Mozilla Firefox 代码执行漏洞（CNVD-2018-13863、CNVD-2018-13891）、Mozilla Firefox 越权漏洞”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-2018-13663

http://www.cnvd.org.cn/flaw/show/CNVD-2018-13662

http://www.cnvd.org.cn/flaw/show/CNVD-2018-13863

http://www.cnvd.org.cn/flaw/show/CNVD-2018-13885

http://www.cnvd.org.cn/flaw/show/CNVD-2018-13891

http://www.cnvd.org.cn/flaw/show/CNVD-2018-13890

http://www.cnvd.org.cn/flaw/show/CNVD-2018-13964

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14109

5、D-Link DAP-1360 文件路径遍历和跨站脚本漏洞

D-Link DAP-1360 是一款无线路由器。本周，Cisco UCS Software 被披露存在文件路径遍历和跨站脚本漏洞，远程攻击者通过错误的参数读取密码，导致绝对路径遍历攻击。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-2018-13970

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-2018-13652	RSA Archer REST API 授权绕过漏洞	高	用户可联系供应商获得补丁信息：http://www.emc.com/products/security/product-security-response-center.htm
CNVD-2018-13652	RSA Archer REST API 授权绕过漏洞	高	用户可联系供应商获得补丁信息：http://www.emc.com/products/security/product-security-response-center.htm
CNVD-2018-13653	RSA Archer 跨站脚本漏洞	高	用户可联系供应商获得补丁信息：http://www.emc.com/products/security/product-security-response-center.htm
CNVD-2018-13758	Dell EMC XML 外部实体注入漏洞	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.dellemc.com
CNVD-2018-13764	Etere EtereWeb SQL 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.etere.com/
CNVD-2018-13781	多款 Advantech 产品堆缓冲区溢出漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：http://support.advantech.com/support/DownloadSRDetail_New.aspx?SR_ID=1-MS9MJV&Doc_Source=Download
CNVD-2018-13868	QNAP QTS LDAP Server 命令注入漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.qnap.com/en/security-advisory/nas-201806-19
CNVD-2018-13896	Trovebox SQL 注入漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://github.com/photo/frontend
CNVD-2018-13993	Citrix NetScaler Application Delivery Controller 和 NetScaler Gateway 任意代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://support.citrix.com/article/CTX234869
CNVD-2018-14072	Intel Converged Security Management Engine 缓冲区溢出漏洞	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.intel.com/content/www/us/en/security-center/advisory/intel-sa-00112.html
CNVD-2018-14071	Intel Converged Security Management Engine 任意代码执行漏洞	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.intel.com/content/www/us/en/security-center/advisory/intel-sa-00118.html

小结：本周，Cisco 被披露存在多个漏洞，攻击者可利用漏洞执行任意代码或发起

拒绝服务攻击。此外，Foxit、IBM、Mozilla 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，读取任意文件，执行任意代码或发起拒绝服务攻击等。另外，D-Link DAP-1360 存在文件路径遍历和跨站脚本漏洞，远程攻击者通过错误的参数读取密码，导致绝对路径遍历攻击。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. 大量蓝牙设备和系统将受加密漏洞

近期，安全研究专家在某些蓝牙设备中发现了一个高危加密漏洞（CVE-2018-5383），未经验证的攻击者在物理接近目标设备后，将允许他们拦截、监控或篡改设备的网络数据。受影响的包括苹果、博通、英特尔和高通等大型厂商所生产的设备固件以及操作系统软件驱动器，另外该漏洞是否会影响 Android 和 Linux 设备，目前还是未知数。该漏洞主要会影响两种蓝牙功能，第一个是操作系统软件中用于安全连接配对的低功耗蓝牙（LE）实现，第二个是设备固件中用于安全简单配对的 BR/EDR 实现。

参考链接：http://www.freebuf.com/news/178833.html

2. WebLogic 两处任意文件上传漏洞动态分析

前几天，Oracle 公司出品的基于 JavaEE 结构的中间件 WebLogic 产品存在一个远程上传漏洞，并得到了厂商的确认，危害程度评分高达 9.8 分。WebLogic 管理端未授权的两个页面存在任意上传 getshell 漏洞，可直接获取权限。两个页面分别为/ws_utc/begin.do，/ws_utc/config.do；漏洞的影响范围 Oracle WebLogic Server，版本 10.3.6.0，12.1.3.0，12.2.1.2，12.2.1.3。

参考链接：http://www.freebuf.com/vuls/178510.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