国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2018 年 9 月 3 日-2018 年 9 月 9 日 **2018 年第 36 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 424 个，其中高危漏洞 177 个、中危漏洞 221 个、低危漏洞 26 个。漏洞平均分值为 6.21。本周收录的漏洞中，涉及 0day 漏洞 93 个（占 22%），其中互联网上出现“QNAP Q'center Virtual Appliance 命令注入漏洞（CNVD-2018-17532）、WordPress Gift Vouchers SQL 注入漏洞”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 711 个，与上周（879 个）环比下降 19%。

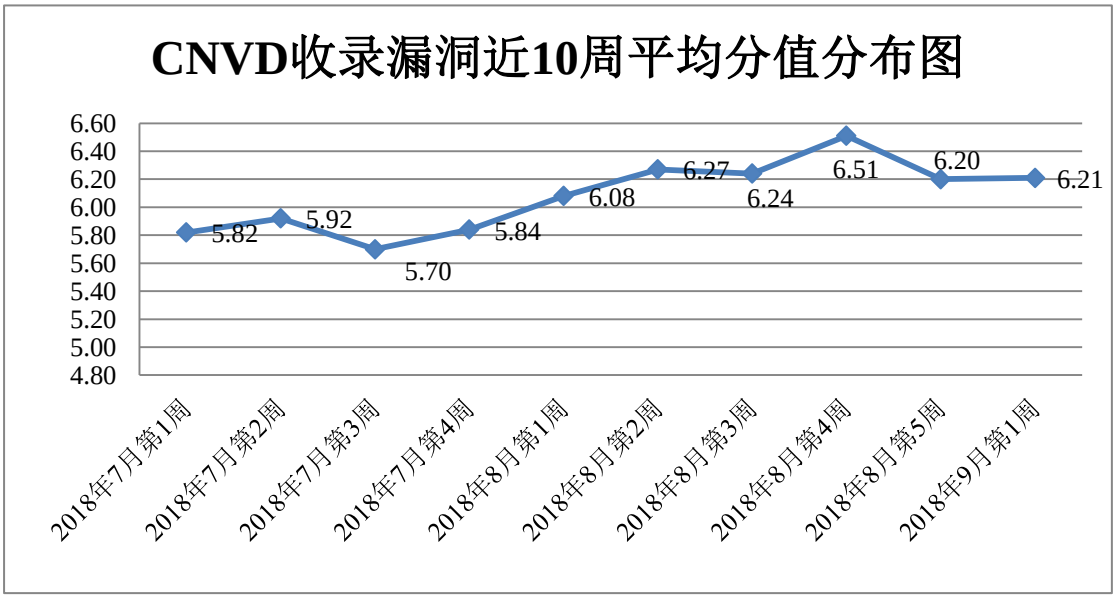

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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、北京知道创宇信息技术有限公司、新华三技术有限公司、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、北京圣博润高新技术股份有限公司、中新网络信息安全股份有限公司、南京联成科技发展股份有限公司、北京智游网安科技有限公司、四川虹微技术有限公司（子午攻防实验室）、任子行网络技术股份有限公司、北京明朝万达科技股份有限公司（安元实验室）、上海银基信息安全技术股份有限公司及其他个人白帽子向 CNVD 提交了 711 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 253 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	285	1
哈尔滨安天科技股份有限公司	218	0
北京知道创宇信息技术有限公司	205	203
360 网神（补天平台）	205	205
新华三技术有限公司	205	0
华为技术有限公司	176	0
北京数字观星科技有限公司	93	0
北京神州绿盟科技有限公司	66	0
中国电信集团系统集成有限责任公司	61	1
恒安嘉新(北京)科技股份公司	55	0
北京启明星辰信息安全技术有限公司	51	6
漏洞盒子	48	48
北京无声信息技术有限公司	28	26
深圳市深信服电子科技有限公司	18	0
厦门服云信息科技有限公司	11	0
山东云天安全技术有限公司	78	78

北京圣博润高新技术股份有限公司	29	29
中新网络信息安全股份有限公司	8	8
南京联成科技发展股份有限公司	7	7
北京智游网安科技有限公司	5	5
四川虹微技术有限公司（子午攻防实验室）	4	4
任子行网络技术股份有限公司	2	2
北京明朝万达科技股份有限公司（安元实验室）	1	1
上海银基信息安全技术股份有限公司	1	1
CNCERT 新疆分中心	5	5
CNCERT 上海分中心	2	2
CNCERT 海南分中心	1	1
CNCERT 湖南分中心	1	1
CNCERT 天津分中心	1	1
个人	76	76
报送总计	1946	711

本周漏洞按类型和厂商统计

本周，CNVD 收录了 424 个漏洞。应用程序漏洞 212 个，WEB 应用漏洞 155 个，网络设备漏洞 38 个，安全产品漏洞 11 个，操作系统漏洞 8 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	212
WEB 应用漏洞	155
网络设备漏洞	38
安全产品漏洞	11
操作系统漏洞	8

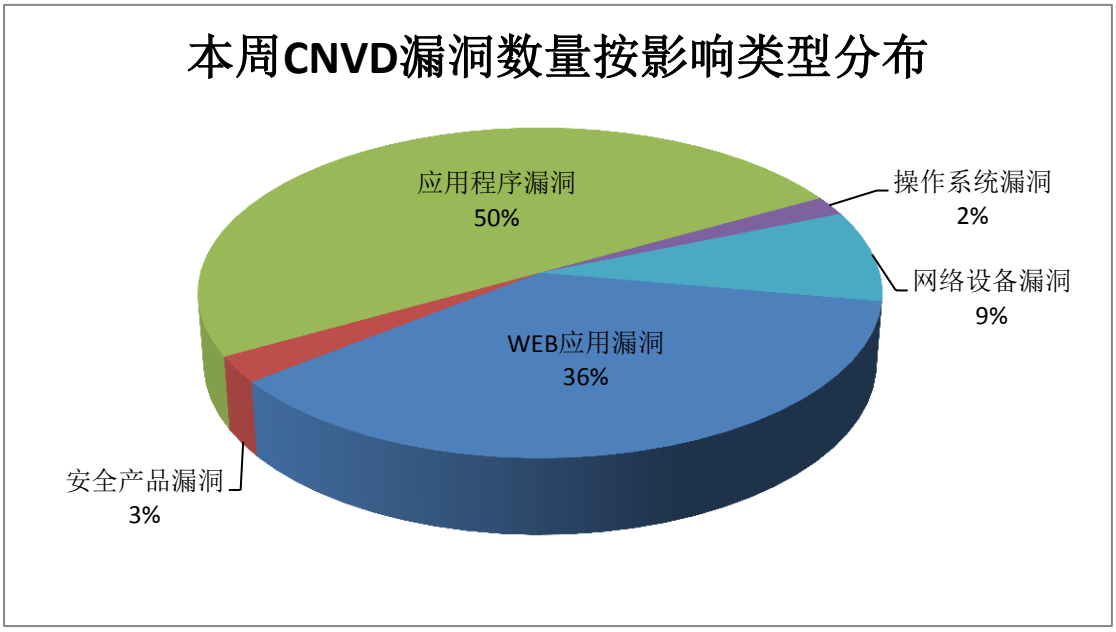

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Red Hat、Cisco、广州国微软件科技有限公司等多家厂商的产品，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	Red Hat	26	6%
2	Cisco	12	3%
3	广州国微软件科技有限公司	12	3%
4	Microsoft	11	3%
5	Dell	9	2%
6	Atlassian	8	2%
7	Apple	6	1%
8	IBM	6	1%
9	CA	6	1%
10	其他	328	78%

本周行业漏洞收录情况

本周，CNVD 收录了 16 个电信行业漏洞，25 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，“LiteCart 文件上传漏洞、OURPHP 建站系统 V1.8.3 存在逻辑漏洞、和利时 PLC LE5109L 存在远程控制漏洞” 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/

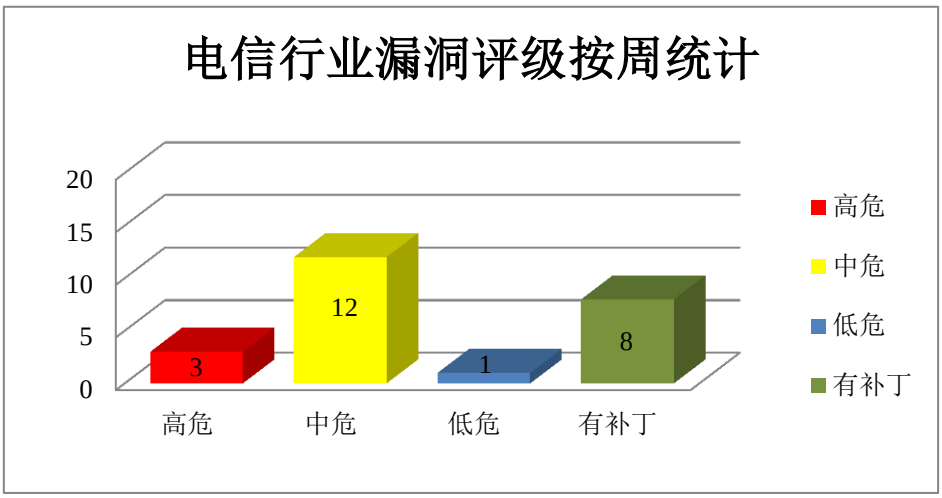

图 3 电信行业漏洞统计

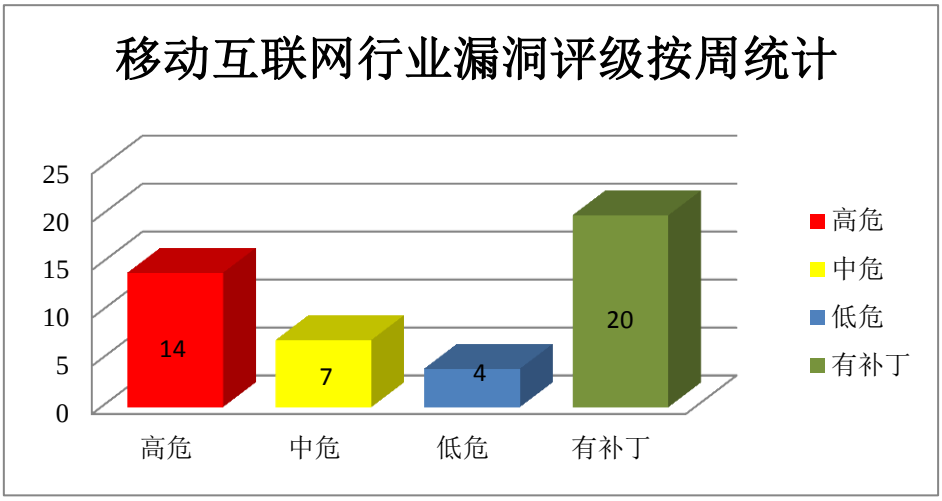

图 4 移动互联网行业漏洞统计

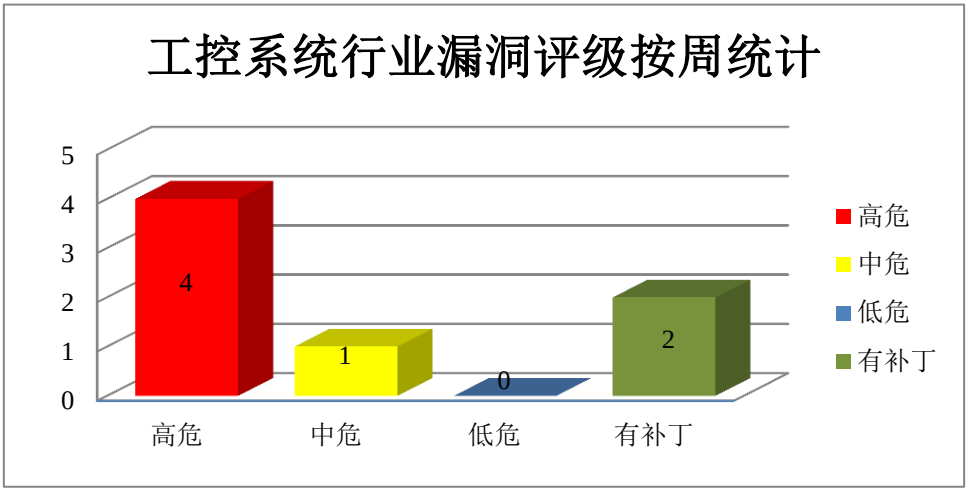

图 5 工控系统行业漏洞统计

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、Red Hat 产品安全漏洞

Red Hat OpenShift 是一款平台即服务（PaaS）云计算平台。openshift-ansible 是其中的一个用于安装、升级和管理 OpenShift 的工具。Red Hat 389-ds-base 是包括了 Linux 目录服务器和服务器管理命令行程序的软件包。Red Hat RPM（RPM Package Manager）是一款命令行驱动的软件包管理器。Red Hat glusterfs server 是一套开源的分布式文件系统。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，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：Red Hat openshift-ansible SSL 客户端证书身份验证漏洞、Red Hat 389-ds-base 竞争条件漏洞、Red Hat 389-ds-base 信息泄露漏洞、Red Hat RPM 权限提升漏洞（CNVD-2018-17735）、Red Hat glusterfs 服务器 RPC 请求处理器组件权限提升漏洞、Red Hat glusterfs 服务器 RPC 请求处理器组件任意文件创建漏洞、Red Hat glusterfs 服务器远程代码执行漏洞、Red Hat glusterfs 服务器反序列化漏洞。其中，除“Red Hat 389-ds-base 信息泄露漏洞”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-2018-17718
http://www.cnvd.org.cn/flaw/show/CNVD-2018-17720
http://www.cnvd.org.cn/flaw/show/CNVD-2018-17723
http://www.cnvd.org.cn/flaw/show/CNVD-2018-17735
http://www.cnvd.org.cn/flaw/show/CNVD-2018-17744
http://www.cnvd.org.cn/flaw/show/CNVD-2018-17745
http://www.cnvd.org.cn/flaw/show/CNVD-2018-17758
http://www.cnvd.org.cn/flaw/show/CNVD-2018-17759

2、Microsoft 产品安全漏洞

Microsoft Office PowerPoint 是微软公司的演示文稿软件。Microsoft Edge 是一款 Web 浏览器。ChakraCore 是使用在其中的一个开源的 Chakra JavaScript 脚本引擎的核心部分，也可作为单独的 JavaScript 引擎使用。Microsoft Windows 10 是一套个人电脑使用的操作系统。Windows Server 2016 是一套服务器操作系统。Internet Explorer（IE）是其中的一款 Windows 操作系统附带的 Web 浏览器。本周，上述产品被披露存在内存破坏和远程代码执行漏洞，攻击者可利用漏洞执行任意代码，破坏内存。

CNVD 收录的相关漏洞包括：Microsoft PowerPoint 远程代码执行漏洞（CNVD-2018-17618）、Microsoft Edge 远程代码执行漏洞（CNVD-2018-18003）、Microsoft Interne

t Explorer 远程代码执行漏洞（CNVD-2018-18005）、Microsoft Edge 远程代码执行漏洞（CNVD-2018-18004）、Microsoft Edge Chakra 脚本引擎远程内存破坏漏洞、Microsoft ChakraCore 远程代码执行漏洞（CNVD-2018-18047）、Microsoft ChakraCore 和 Edge 内存破坏漏洞、Microsoft Edge 和 ChakraCore 远程内存破坏漏洞（CNVD-2018-18049）。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-2018-17618

http://www.cnvd.org.cn/flaw/show/CNVD-2018-18003

http://www.cnvd.org.cn/flaw/show/CNVD-2018-18005

http://www.cnvd.org.cn/flaw/show/CNVD-2018-18004

http://www.cnvd.org.cn/flaw/show/CNVD-2018-18045

http://www.cnvd.org.cn/flaw/show/CNVD-2018-18047

http://www.cnvd.org.cn/flaw/show/CNVD-2018-18048

http://www.cnvd.org.cn/flaw/show/CNVD-2018-18049

3、Dell 产品安全漏洞

Dell RSA Identity Lifecycle and Governance 是一套身份治理和生命周期管理解决方案。Dell EMC iDRAC9 是一套包含硬件和软件的系统管理解决方案。Dell EMC iDRAC6 是包含硬件和软件的系统管理解决方案。Dell RSA Identity Governance and Lifecycle 是一套生命周期管理解决方案；RSA Via Lifecycle and Governance 是一套企业级身份识别和管理解决方案；RSA IMG 是一套生命周期管理和身份识别解决方案。Dell EMC RSA BSAFE Micro Edition Suite（MES）和 RSA BSAFE Crypto-C Micro Edition 都是加密工具包。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞对用户会话实施暴力破解攻击，获取未授权数据的访问权限，执行恶意 HTML 或 JavaScript 代码，发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Dell RSA Identity Governance and Lifecycle 跨站脚本漏洞、Dell EMC iDRAC9 SSL/TLS 保护剥离漏洞、多款 Dell 产品暴力破解漏洞、Dell RSA Identity Governance and Lifecycle、RSA Via Lifecycle and Governance 和 RSA IMG 本地不可信搜索路径漏洞、Dell EMC RSA BSAFE Micro Edition Suite 整数溢出漏洞、Dell EMC RSA BSAFE Micro Edition Suite 内存错误引用漏洞、Dell EMC RSA BSAFE Micro Edition Suite 和 RSA BSAFE Crypto-C Micro Edition 资源耗尽漏洞、Dell EMC RSA BSAFE Micro Edition Suite 隐蔽定时信道漏洞。其中，“Dell RSA Identity Governance and Lifecycle、RSA Via Lifecycle and Governance 和 RSA IMG 本地不可信搜索路径漏洞、Dell EMC RSA BSAFE Micro Edition Suite 整数溢出漏洞、Dell EMC RSA BSAFE Micro Edition Suite 内存错误引用漏洞、Dell EMC RSA BSAFE Micro Edition Suite 和 RSA BSAFE Crypto-C Micro Edition 资源耗尽漏洞”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-2018-17474

http://www.cnvd.org.cn/flaw/show/CNVD-2018-17691

http://www.cnvd.org.cn/flaw/show/CNVD-2018-17692

http://www.cnvd.org.cn/flaw/show/CNVD-2018-17690

http://www.cnvd.org.cn/flaw/show/CNVD-2018-17693

http://www.cnvd.org.cn/flaw/show/CNVD-2018-17694

http://www.cnvd.org.cn/flaw/show/CNVD-2018-17695

http://www.cnvd.org.cn/flaw/show/CNVD-2018-17696

4、Cisco 产品安全漏洞

Cisco Webex Teams 是一款团队协作应用程序。Umbrella Roaming 是一款防火墙的云端安全服务。Cisco 3000 Series Industrial Security Appliances（ISR）等都是安全防火墙设备。Adaptive Security Appliance（ASA）和 Firepower Threat Defense（FTD）Software 都是使用在 Cisco 不同安全设备中的防火墙软件。Cisco RV110W、RV130W 和 RV215W 均为路由器产品。Cisco WebEx Meetings 是网络会议解决方案。Cisco Identity Services Engine（ISE）是一款基于身份的环境感知平台（ISE 身份服务引擎）。Cisco AMP for Endpoints Mac Connector Software for macOS 是一套基于 macOS 平台的集成了静态和动态恶意软件分析以及威胁情报于一体的终端应用程序。Cisco IOS XR for Cisco ASR 9000 Series Aggregation Services Routers 是一套运行于 9000 系列路由器设备中的操作系统。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞查看和修改敏感信息，提升权限，执行任意代码或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Cisco Webex Teams 信息泄露和修改漏洞、Cisco Umbrella Enterprise Roaming Client and Enterprise Roaming Module 权限提升漏洞、Cisco 多款路由器管理接口缓冲区溢出漏洞、Cisco Webex Meetings Client for Windows 权限提升漏洞、多款 Cisco 产品 SSL 证书验证安全绕过漏洞、Cisco Identity Services Engine (ISE)跨站请求伪造漏洞、Cisco AMP for Endpoints macOS Connector 拒绝服务漏洞、Cisco ASR 9000 Series Aggregation Services Routers 本地拒绝服务漏洞。其中，“Cisco Webex Teams 信息泄露和修改漏洞、Cisco 多款路由器管理接口缓冲区溢出漏洞、Cisco Webex Meetings Client for Windows 权限提升漏洞”的综合评级为“高危”。目前，除“Cisco 多款路由器管理接口缓冲区溢出漏洞、Cisco Webex Meetings Client for Windows 权限提升漏洞”外，厂商已经发布其余漏洞的修补程序。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-2018-17680

http://www.cnvd.org.cn/flaw/show/CNVD-2018-17679

http://www.cnvd.org.cn/flaw/show/CNVD-2018-17682

http://www.cnvd.org.cn/flaw/show/CNVD-2018-17681

http://www.cnvd.org.cn/flaw/show/CNVD-2018-17707

http://www.cnvd.org.cn/flaw/show/CNVD-2018-17708

http://www.cnvd.org.cn/flaw/show/CNVD-2018-17709

http://www.cnvd.org.cn/flaw/show/CNVD-2018-17712

5、SAP Business Objects 远程代码注入漏洞

SAP Business Objects 是一套商务智能软件和企业绩效解决方案。该方案提供报表、绩效管理和数据基础等功能。本周，SAP Business Objects 被披露存在远程代码注入漏洞。攻击者可以利用漏洞注入远程代码，在服务器上执行任意命令。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-2018-17535

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-2018-17414	多款 Micro Focus 产品代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://softwaresupport.softwaregrp.com/document/-/facetsearch/document/KM03236632
CNVD-2018-17506	IBM Maximo Asset Management 权限获取漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www-01.ibm.com/support/docview.wss?uid=swg22017452
CNVD-2018-17644	Atlassian Sourcetree for Windows 参数注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://jira.atlassian.com/browse/SRCTREEWIN-8884
CNVD-2018-17656	F5 BIG-IP 拒绝服务漏洞（CNVD-2018-17656）	高	厂商已发布了漏洞修复程序，请及时关注更新：http://support.f5.com/csp/article/K20134942
CNVD-2018-17667	Apple macOS High Sierra APFS 组件权限提升漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.apple.com/en-us/HT208937
CNVD-2018-17896	A10 ACOS Web Application Firewall SQL 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://www.a10networks.com/support/security-advisories/waf-sql-injection-attack-sqlia-vulnerability
CNVD-2018-17897	ASUSTOR Data Master 路径遍历漏洞（CNVD-2018-17897）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.asustor.com/
CNVD-2018-17906	Umbraco 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://issues.umbraco.org/issue/U4-5901
CNVD-2018-17907	Lansweeper 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：https://www.lansweeper.com/updates/lansweeper-6-0-0-48-security-update/
CNVD-2018-17999	Trend Micro Control Manager 路径遍历漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://success.trendmicro.com/solution/1120112

小结：本周， Red Hat 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，执行任意代码或发起拒绝服务攻击。此外，Microsoft、Dell、Cisco 等多款产品被披露存在多个漏洞，攻击者可利用漏洞对用户会话实施暴力破解攻击，查看和修改敏感信息，提升权限，执行任意代码，破坏内存或发起拒绝服务攻击等。另外，SAP Business Objects 被披露存在远程代码注入漏洞。攻击者可以利用漏洞注入远程代码，在服务器上执行任意命令。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. Android 系统广播机制存在漏洞，恶意软件可绕过安全机制跟踪用户

近日，国外研究人员披露了 Android 漏洞（CVE-2018-9489）的信息。Android 系统的内部广播机制会暴露敏感的用户和设备信息，手机上安装的应用可在用户不知情或未经许可的情况下访问获取这些信息。Android 系统的内部广播机制泄露的数据包括：Wi-Fi 网络名称、Wi-Fi 网络 BSSID，本地 IP 地址、DNS 服务器信息和设备的 MAC 地址等详细信息。部分信息（如 Mac 地址）在 Android 6 版本以上无法通过这个漏洞获取，但是剩下的依然可以通过监听广播来绕过权限检查和其他防范措施。

参考链接：http://www.freebuf.com/news/182795.html

2. ECShop 2.x 和 3.0 版本代码执行漏洞

ECShop 是一款 B2C 独立网店系统，适合企业及个人快速构建个性化网上商店。2.x 版本跟 3.0 版本存在代码执行漏洞。ECShop 未能对 $GLOBAL[‘_SERVER’][‘HTTP_REFERER’] 变量进行验证，导致用户可以将任意代码插入的 user_passport.dwt 模板中，随后 insert_mod 根据模板内容动态执行相应的函数，用户插入恶意代码导致模板

动态执行了 lib_insert 下的 insert_ads 方法，通过 SQL 注入，返回构造的执行代码，致使后面调用 cls_template 模板类的 fetch 函数，成功执行恶意代码。

参考链接：http://www.freebuf.com/vuls/183294.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