国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2018 年 11 月 12 日-2018 年 11 月 18 日 **2018 年第 46 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 202 个，其中高危漏洞 100 个、中危漏洞 81 个、低危漏洞 21 个。漏洞平均分值为 6.53。本周收录的漏洞中，涉及 0day 漏洞 82 个（占 41%），其中互联网上出现“ZyXEL ZyWALL USG 跨站请求伪造漏洞、Nagios XI 任意命令执行漏洞”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 1289 个，与上周（1228 个）环比增长 5%。

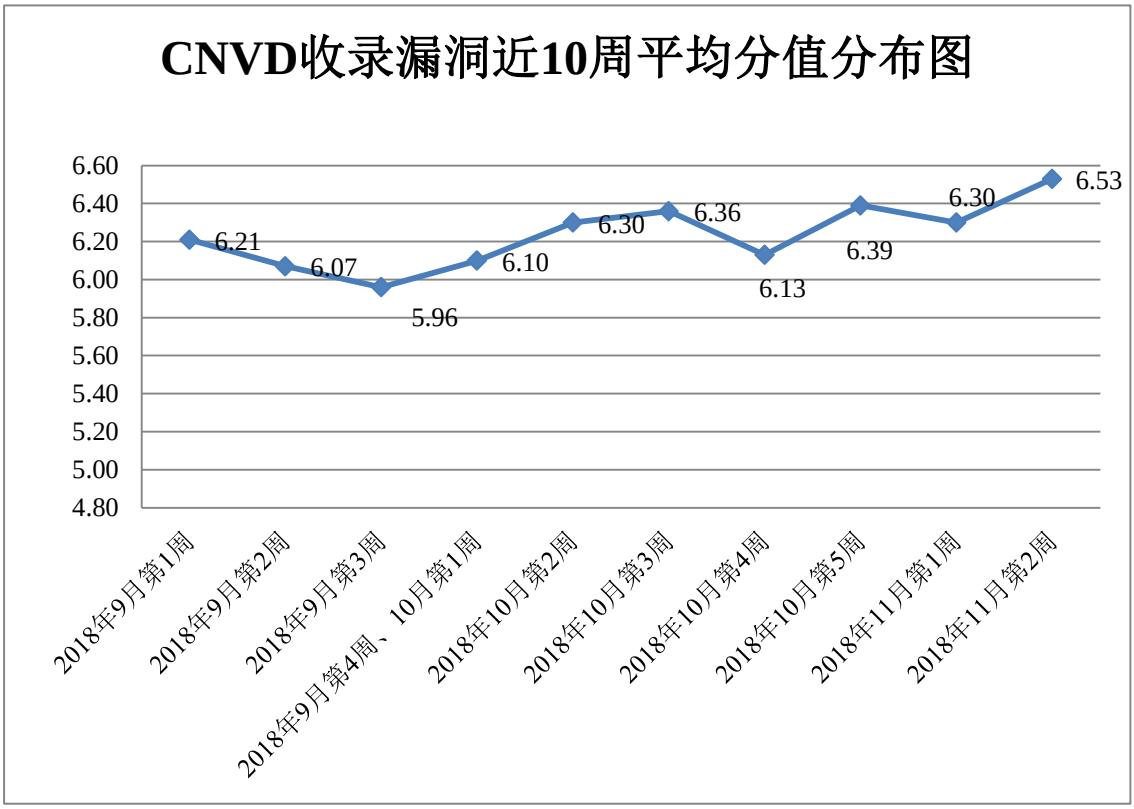

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 4 起，向银行、证券、保险、能源等重要行业单位通报漏洞事件 26 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 238 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 141 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 32 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：

长沙米拓信息技术有限公司、金山软件股份有限公司、北京拓敏信息技术有限公司、广州七侠旅行社有限公司、天津触网科技有限公司、上海浪擎信息科技有限公司、深圳市科脉技术股份有限公司、中国电建集团华东勘测设计研究院有限公司、南昌蓝智科技有限公司、厦门凤凰创壹软件有限公司、海南易联众信息技术有限公司、镇江市云优网络科技有限公司、上海七慧网络科技有限公司、深圳市远扬航空货运有限公司、太原飞扬动力科技有限公司、辽源市公共汽车公司、漳州豆壳网络科技有限公司、沧州市凡诺广告传媒有限公司、宜软通网、新京报网、预告中文网、易贝软件、崇胜网络科技、蓝科外贸网站、中国消费者协会、雷风影视、优客 365、中国化学工程学报、UCMS、ZZCMS、EARCLINK、老班 cms、YCCMS。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，沈阳东软系统集成工程有限公司、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、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、南京联成科技发展股份有限公司、远江盛邦（北京）网络安全科技股份有限公司、中新网络信息安全股份有限公司、河北盾安科技有限公司、北京国舜科技股份有限公司、任子行网络技术股份有限公司、上海启疆信息科技有限公司、内蒙古奥创科技有限公司、浙江鹏信信息科技股份有限公司、山石网科通信技术有限公司、北京长亭科技有限公司、广州竞远安全技术股份有限公司及其他个人白帽子向 CNVD 提交了 1289 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 976 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
360 网神（补天平台）	746	746

沈阳东软系统集成工程有限公司	495	0
北京天融信网络安全技术有限公司	283	5
漏洞盒子	230	230
哈尔滨安天科技股份有限公司	205	0
新华三技术有限公司	171	0
华为技术有限公司	98	0
深信服科技股份有限公司	87	0
中国电信集团系统集成有限责任公司	61	0
北京神州绿盟科技有限公司	56	0
北京启明星辰信息安全技术有限公司	56	7
北京数字观星科技有限公司	51	0
恒安嘉新(北京)科技股份公司	50	1
北京知道创宇信息技术有限公司	4	0
山东云天安全技术有限公司	98	98
北京圣博润高新技术股份有限公司	23	23
南京联成科技发展股份有限公司	9	9
远江盛邦（北京）网络安全科技股份有限公司	8	8
中新网络信息安全股份有限公司	8	8
河北盾安科技有限公司	6	6
北京国舜科技股份有限公司	3	3
任子行网络技术股份有限公司	3	3
上海启疆信息科技有限公司	3	3

内蒙古奥创科技有限公司	2	2
浙江鹏信信息科技股份有限公司	2	2
山石网科通信技术有限公司	1	1
北京长亭科技有限公司	1	1
广州竞远安全技术股份有限公司	1	1
CNCERT 甘肃分中心	5	5
CNCERT 海南分中心	5	5
CNCERT 上海分中心	2	2
CNCERT 河北分中心	1	1
CNCERT 湖南分中心	1	1
个人	118	118
报送总计	2893	1289

本周漏洞按类型和厂商统计

本周，CNVD 收录了 202 个漏洞。应用程序漏洞 109 个，WEB 应用漏洞 55 个，操作系统漏洞 27 个，网络设备漏洞 8 个，安全产品漏洞 2 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	109
WEB 应用漏洞	55
操作系统漏洞	27
网络设备漏洞	8
安全产品漏洞	2
数据库漏洞	1

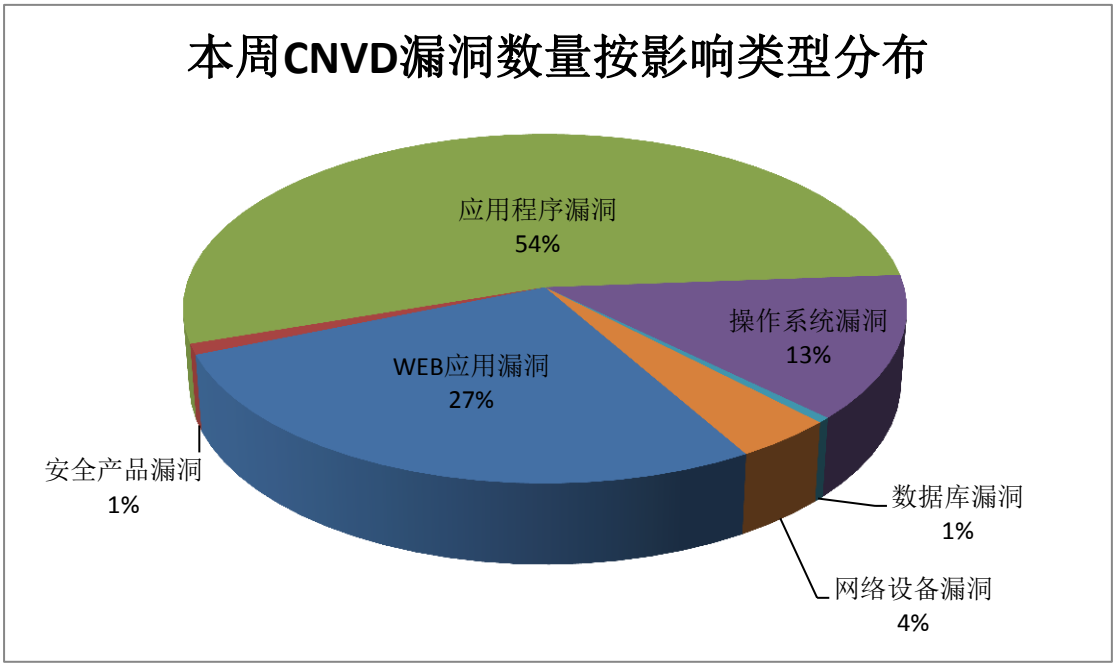

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Foxit、Apple、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	Foxit	20	10%
2	Apple	19	10%
3	IBM	17	8%
4	Microsoft	17	8%
5	LAOBANCMS	9	5%
6	Broadcom	8	4%
7	镇江市云优网络科技有限公司	7	3%
8	Nagios	6	3%
9	WordPress	5	2%
10	其他	94	47%

本周行业漏洞收录情况

本周，CNVD 收录了 9 个电信行业漏洞，4 个移动互联网行业漏洞，2 个工控行业漏洞（如下图所示）。其中，“Brocade Fabric OS 任意命令执行漏洞、Brocade Fabric OS 安全绕过漏洞、Brocade Fabric OS 权限提升漏洞”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/

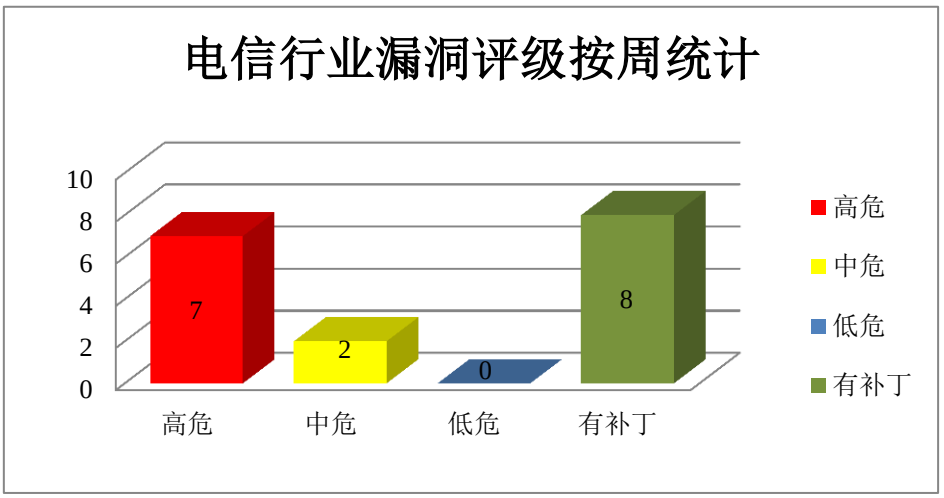

图 3 电信行业漏洞统计

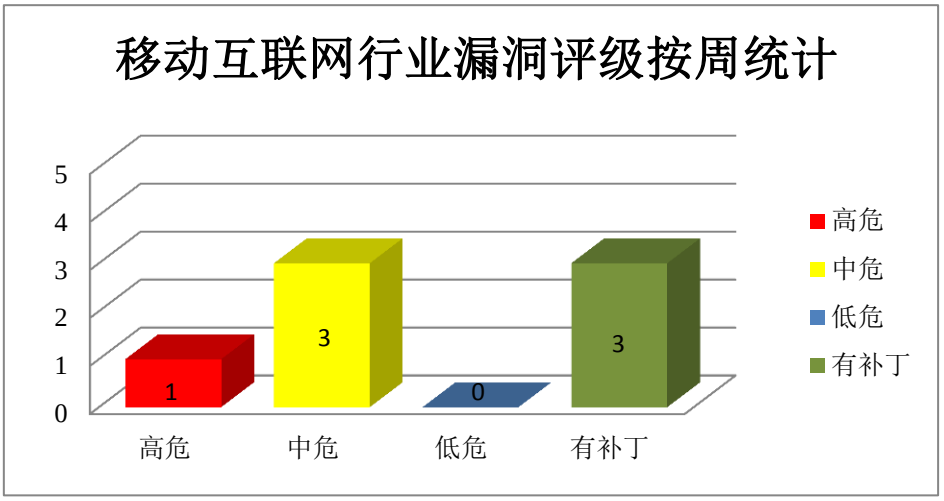

图 4 移动互联网行业漏洞统计

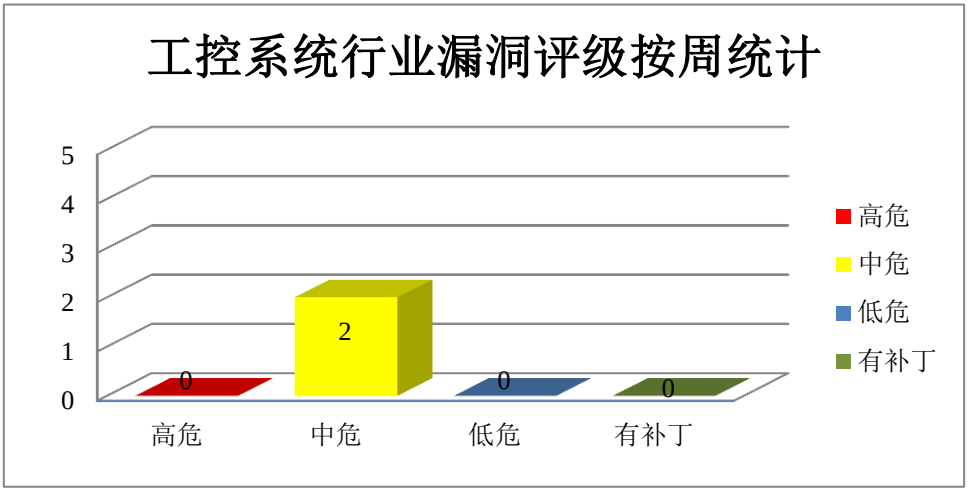

图 5 工控系统行业漏洞统计

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-2018-23229、CNVD-2018-23231、CNVD-2018-23232、CNVD-2018-23230、CNVD-2018-23233、CNVD-2018-23234、CNVD-2018-23235、CNVD-2018-23236）。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-2018-23229

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23231

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23232

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23230

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23233

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23234

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23235

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23236

2、Apple 产品安全漏洞

macOS 是苹果公司为 Mac 系列产品开发的专属操作系统。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，导致堆破坏。

CNVD 收录的相关漏洞包括：Apple macOS 内存破坏漏洞（CNVD-2018-22950、CNVD-2018-22952、CNVD-2018-22951、CNVD-2018-22953、CNVD-2018-22955、CNVD-2018-22954、CNVD-2018-22956、CNVD-2018-22958）。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-2018-22950

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22952

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22951

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22953

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22955

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22954

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22956

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22958

3、IBM 产品安全漏洞

IBM Maximo Asset Management 是一套综合性资产生命周期和维护管理解决方案。IBM Rational Collaborative Lifecycle Management（CLM）是一套协作化生命周期管理解决方案。IBM Rational Quality Manager（RQM）是一套协作的、基于 Web 的质量管理解决方案。IBM WebSphere MQ Managed File Transfer 是其中的一个用于管理系统中文件传输的工具。IBM MQ(前称 IBM WebSphere MQ)是一款消息传递中间件产品。IBM Security Identity Governance and Intelligence Virtual Appliance 是一套身份管理和治理解决方案。IBM API Connect 是一种综合的端到端 API 生命周期解决方案。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 Maximo Asset Management 跨站脚本漏洞（CNVD-2018-23091）、IBM Jazz Foundation 信息泄露漏洞（CNVD-2018-23241）、多款 IBM Rational 产品信息泄露漏洞（CNVD-2018-23242）、IBM WebSphere MQ Managed File Transfer 信息泄露漏洞、IBM MQ 拒绝服务漏洞、IBM Security Identity Governance and Intelligence Virtual Appliance 信息泄露漏洞、IBM API Connect 信息泄露漏洞、IBM Rational Quality Manager 权限提升漏洞。其中，“IBM Rational Quality Manager 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-2018-23091

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23241

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23242

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23243

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23246

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23245

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23252

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23253

4、Microsoft 产品安全漏洞

Edge 是微软为 Windows 10 打造的浏览器。本周，该产品被披露存在信息泄露和内存破坏漏洞，攻击者可利用漏洞获取敏感信息，执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Edge Chakra 脚本引擎内存破坏漏洞（CNVD-2018-23213、CNVD-2018-23216、CNVD-2018-23215、CNVD-2018-23217、CNVD-2018-23218、CNVD-2018-23262、CNVD-2018-23263）、Microsoft Edge 信息泄露漏洞（CNVD-2018-23281）。上述漏洞的综合评级为“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-2018-23213
http://www.cnvd.org.cn/flaw/show/CNVD-2018-23216
http://www.cnvd.org.cn/flaw/show/CNVD-2018-23215
http://www.cnvd.org.cn/flaw/show/CNVD-2018-23217
http://www.cnvd.org.cn/flaw/show/CNVD-2018-23218
http://www.cnvd.org.cn/flaw/show/CNVD-2018-23262
http://www.cnvd.org.cn/flaw/show/CNVD-2018-23263
http://www.cnvd.org.cn/flaw/show/CNVD-2018-23281

5、libIEC61850 拒绝服务漏洞

libIEC61850 是一个 IEC 61850 的开源库。本周，libIEC61850 被披露存在拒绝服务漏洞。攻击者可利用该漏洞造成拒绝服务（空指针逆向引用）。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-2018-23028

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-2018-23142	Nagios XI 未授权 API 密钥重新生成漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.nagios.com/downloads/nagios-xi/change-log/
CNVD-2018-22947	VMware ESXi, Workstation and Fusion 未初始化堆栈内存使用漏洞	高	用户可联系供应商获得补丁信息：https://www.vmware.com/security/advisories/VMSA-2018-0027.html
CNVD-2018-23017	CA Privileged Access Manager 身份验证绕过漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://support.ca.com/us/product-content/recommended-reading/security-notices/ca20180614-01--security-notice-for-ca-privileged-access-manager.html
CNVD-2018-23022	McAfee Web Gateway 身份验证绕过漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://kc.mcafee.com/corporate/index?page=content&id=SB10241
CNVD-2018-23026	Gogs 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：https://github.com/zeripath/macaron-session/commit/5d01c1f53f6c5c91b6d7acd81a0736681a131d24

CNVD-2018-23084	Brocade Fabric OS 安全绕过漏洞（CNVD-2018-23084）	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.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2018-731
CNVD-2018-23137	Cybozu Office 目录遍历漏洞（CNVD-2018-23137）	高	用户可联系供应商获得补丁信息：https://cs.cybozu.co.jp/2018/006683.html
CNVD-2018-23139	Cybozu Dezie 目录遍历漏洞	高	用户可联系供应商获得补丁信息：https://cs.cybozu.co.jp/2018/006698.html
CNVD-2018-23141	Nagios XI 权限提升漏洞（CNVD-2018-23141）	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.nagios.com/downloads/nagios-xi/change-log/
CNVD-2018-23140	Nagios XI 任意命令执行漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.nagios.com/downloads/nagios-xi/change-log/

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，Apple、IBM、Microsoft 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，提升权限，执行任意代码或发起拒绝服务攻击等。另外，libIEC61850 被披露存在拒绝服务漏洞。攻击者可利用该漏洞造成拒绝服务（空指针逆向引用）。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、ZyXEL ZyWALL USG 跨站请求伪造漏洞

验证描述

ZyXEL ZyWALL USG 是合勤（ZyXEL）科技公司的一款网络安全防火墙设备。

ZyXEL ZyWALL USG 2.12 AQQ.2 版本和 3.30 AQQ.7 版本中存在跨站请求伪造漏洞。远程攻击者可借助‘cmd’参数利用该漏洞添加用户账户，实施跨站脚本攻击。

验证信息

POC 链接：https://www.shellcode.it/article/cve-2017-17550/

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2018-23092

信息提供者

北京天融信网络安全技术有限公司

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. Gmail 出现漏洞，允许攻击者更改用户表单

近日，软件开发人员发现 Gmail 存在漏洞：在邮件的“发件人”部分，如果使用错误的标题结构则可能导致攻击者在发件人字段中插入任意内容。虽然这个漏洞目前还不会造成太大的危害，但在无形之中增加了网络犯罪的可能性。Cotten 就此事与谷歌进行了联系，目前尚未收到答复。但在上报之后，目前再使用相同的方法进行测试，gmail 会提示有多个地址而无法发送，可以理解为这个漏洞已经被修复了。但使用另一种方式尝试发件依然暴露了类似的问题。

参考链接：https://www.bleepingcomputer.com/news/security/gmail-bugs-allow-changing-from-field-and-spoofing-recipients-address/

2. Oracle 数据库勒索病毒 RushQL 死灰复燃

最近，某终端安全实验室陆续接到数起用户反馈，中了 Oracle 数据库勒索病毒，中毒后的数据库应用界面会弹出下方类似的异常信息。根据此信息，安全实验室确认该病毒是 RushQL 数据库勒索病毒，是由于下载使用了破解版 PL/SQL 导致的。上面的告警声称，病毒是由“SQL RUSH Team”组织发起，因此该病毒被命名为 RushQL。此病毒最早在 2016 年 11 月出现，期间沉寂了 1 年多，直到最近，又陆续接到数起企业、事业单位用户遭受到此病毒的袭击事件，该病毒突然呈现出死灰复燃之势。

参考链接：https://www.anquanke.com/post/id/164570

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