国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2019 年 05 月 20 日-2019 年 05 月 26 日 **2019 年第 21 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 271 个，其中高危漏洞 74 个、中危漏洞 179 个、低危漏洞 18 个。漏洞平均分值为 5.80。本周收录的漏洞中，涉及 0day 漏洞 130 个（占 48%），其中互联网上出现“UCMS SQL 注入漏洞（CNVD-2019-15108）、MacDown 远程代码执行漏洞”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 2475 个，与上周（1672 个）环比增长 48%。

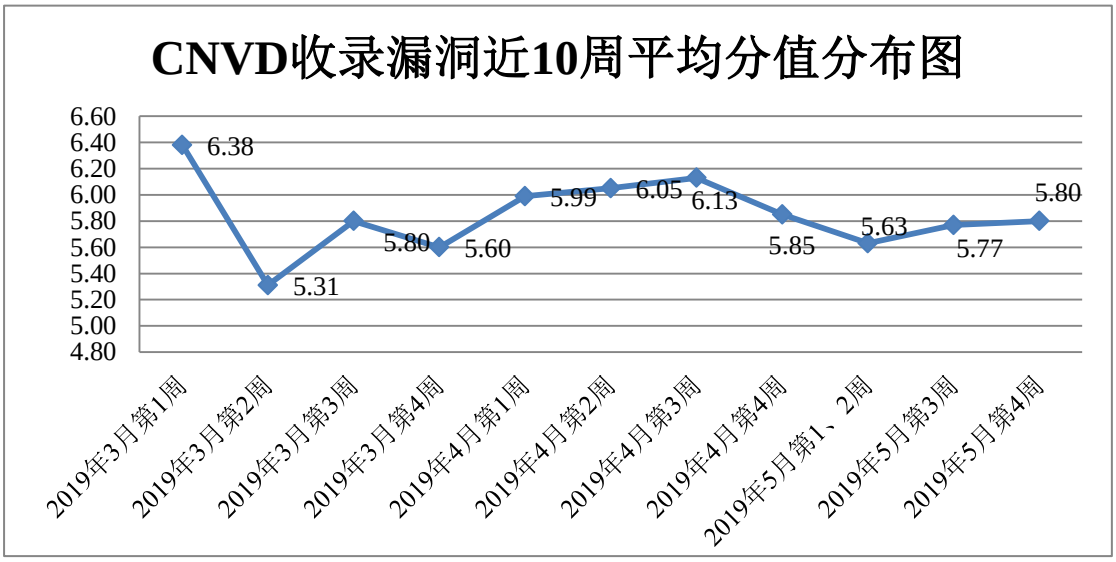

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 10 起，向银行、保险、能源等重要行业单位通报漏洞事件 22 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 267 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 12 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：

深圳搜豹网络有限公司、成都鹏博士电信传媒集团股份有限公司、济南宇霞信息技术有限公司、株洲之窗信息网络文化科技有限公司、北京讯飞乐知行软件有限公司、南京鸣谷科技有限公司、星巴克企业管理（中国）有限公司、浙江齐治科技股份有限公司、沧州市凡诺广告传媒有限公司、北京五指互联科技有限公司、广东盈世计算机科技有限公司、中国高校人文社会科学信息网、宜软通网、施耐德（Schneider Electric）、爱客 CM、易优 CMS、zzzcms、SemCms、SELTECO、astroid、YUNUCM。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，哈尔滨安天科技集团股份有限公司、京天融信网络安全技术有限公司、京启明星辰信息安全技术有限公司、华三技术有限公司、安嘉新(北京)科技股份公司等单位报送公开收集的漏洞数量较多。内蒙古奥创科技有限公司、瑞数码零点实验室、子行网络技术股份有限公司、京铭图天成信息技术有限公司、海并擎软件科技有限公司、京众智维信息科技有限公司、京圣博润高新技术股份有限公司、南信安世纪科技有限公司、东云天安全技术有限公司、国科学院信息工程研究所、山信息科技有限公司及其他个人白帽子向 CNVD 提交了 2475 个以事件型漏洞为主的原创漏洞，其中包括奇安信网神（补天平台）和斗象科技（漏洞盒子）向 CNVD 共享的白帽子报送的 1999 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
斗象科技（漏洞盒子）	1567	1567
奇安信网神（补天平台）	432	432
哈尔滨安天科技集团股份有限公司	218	0
北京天融信网络安全技术有限公司	187	5
北京启明星辰信息安全技术有限公司	150	0
新华三技术有限公司	129	0
恒安嘉新(北京)科技股份公司	123	0

华为技术有限公司	101	0
中国电信集团系统集成有限责任公司	79	0
北京神州绿盟科技有限公司	78	2
深信服科技股份有限公司	73	0
北京数字观星科技有限公司	62	0
四川无声信息技术有限公司	23	23
厦门服云信息科技有限公司	18	0
南京联成科技发展股份有限公司	8	8
北京知道创宇信息技术股份有限公司	5	5
中新网络信息安全股份有限公司	1	1
内蒙古奥创科技有限公司	71	71
国瑞数码零点实验室	70	70
任子行网络技术股份有限公司	60	60
北京铭图天成信息技术有限公司	12	12
上海并擎软件科技有限公司	9	9
南京众智维信息科技有限公司	9	9
北京圣博润高新技术股份有限公司	7	7
河南信安世纪科技有限公司	5	5
山东云天安全技术有限公司	3	3
中国科学院信息工程研究所	1	1
泰山信息科技有限公司	1	1
CNCERT 贵州分中心	4	4

CNCERT 广西分中心	1	1
CNCERT 新疆分中心	1	1
个人	178	178
报送总计	3686	2475

本周漏洞按类型和厂商统计

本周，CNVD 收录了 271 个漏洞。应用程序 193 个，WEB 应用 49 个，网络设备（交换机、路由器等网络端设备）12 个，操作系统 11 个，安全产品 4 个，数据库 1 个，智能设备（物联网终端设备）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	193
WEB 应用	49
网络设备（交换机、路由器等网络端设备）	12
操作系统	11
安全产品	4
数据库	1
智能设备（物联网终端设备）漏洞	1

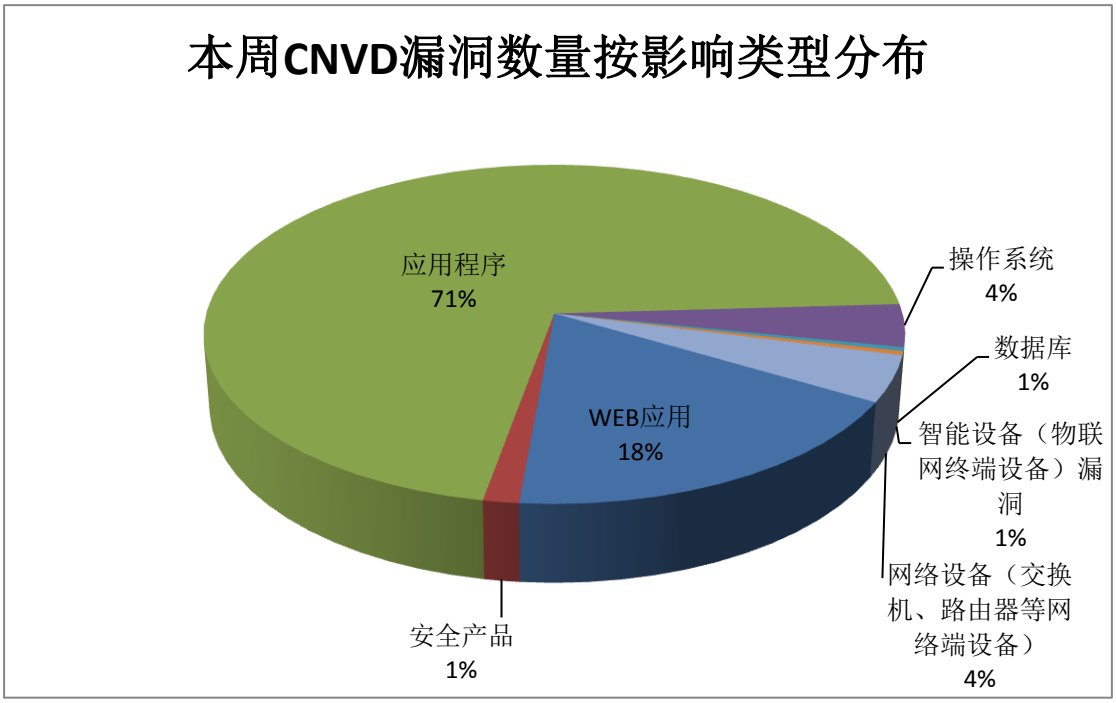

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 CloudBees、Oracle、Google 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	CloudBees	13	5%
2	Oracle	11	4%
3	Google	10	4%
4	GitLab	8	3%
5	Schneider Electric	8	3%
6	Apache	7	3%
7	UltraVNC	7	3%
8	F5	6	2%
9	Atlassian	5	1%
10	其他	196	72%

本周行业漏洞收录情况

本周，CNVD 收录了 6 个电信行业漏洞，17 个移动互联网行业漏洞，26 个工控行业漏洞（如下图所示）。其中，“Samsung Galaxy S9 代码执行漏洞（CNVD-2019-15095）、Google Android System 权限提升漏洞（CNVD-2019-15175）、Siemens SIMATIC PCS 7 和 SIMATIC WinCC 输入验证错误漏洞、Google Android Media framework 权限提升漏洞（CNVD-2019-15201）”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/

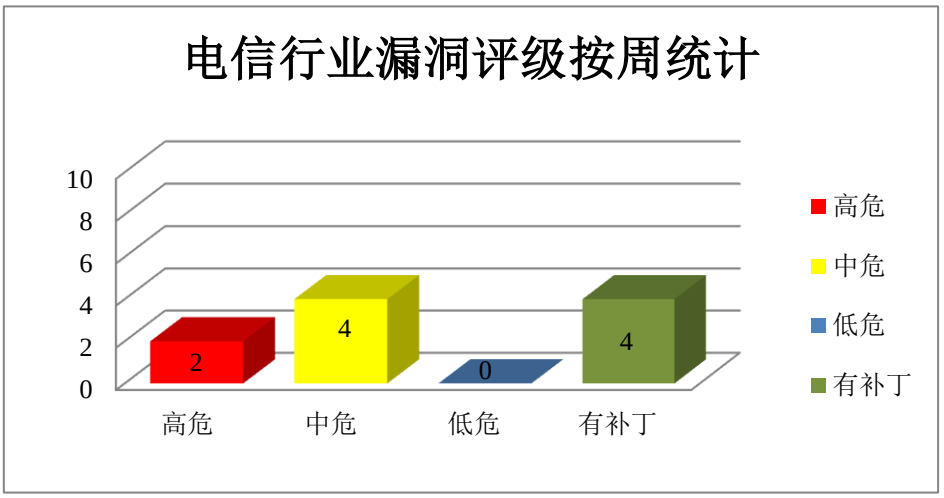

图 3 电信行业漏洞统计

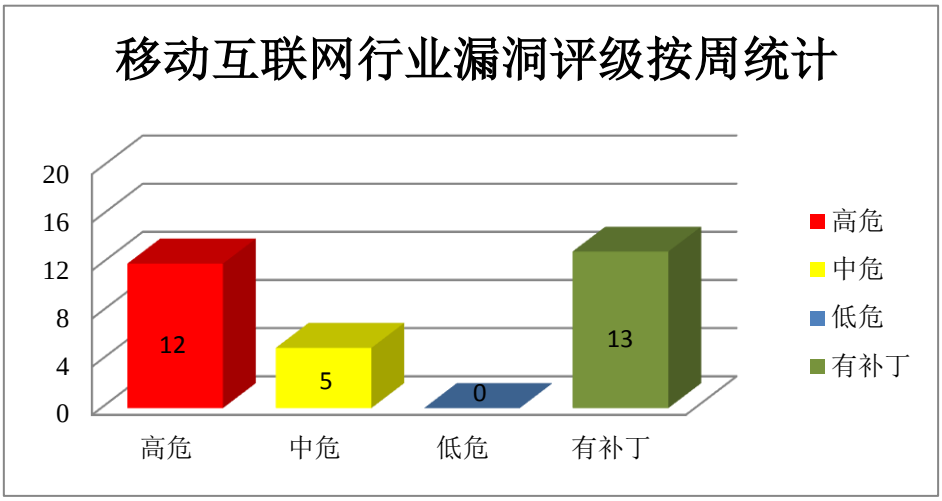

图 4 移动互联网行业漏洞统计

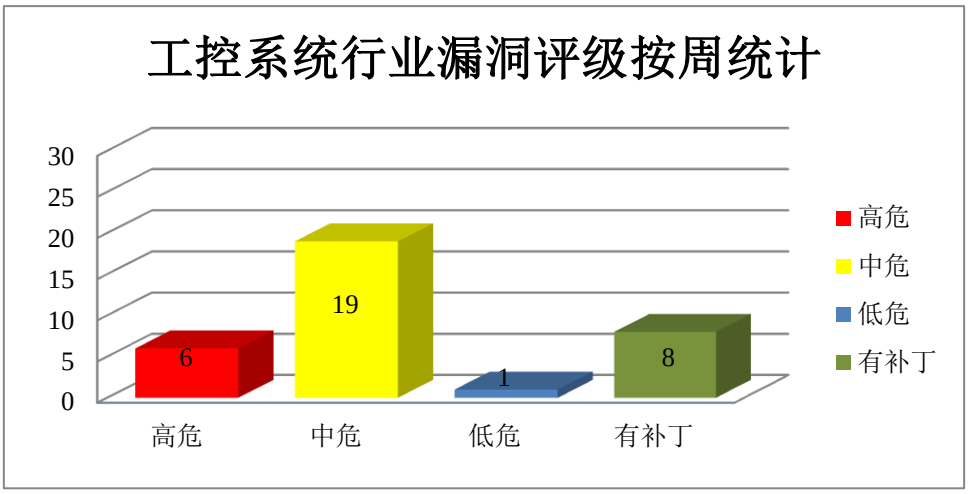

图 5 工控系统行业漏洞统计

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、CloudBees 产品安全漏洞

CloudBees Jenkins（Hudson Labs）是一套基于 Java 开发的持续集成工具。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，绕过沙盒保护，执行任意代码等。

CNVD 收录的相关漏洞包括：CloudBees Jenkins AppDynamics Dashboard Plugin 信任管理问题漏洞、CloudBees Jenkins Azure VM Agents 插件信息泄露漏洞（CNVD-2019-15065）、CloudBees Jenkins Azure VM Agents 插件信息泄露漏洞、CloudBees Jenkins Azure VM Agents 插件权限许可和访问控制漏洞、CloudBees Jenkins Matrix Project Plugin 安全特征问题漏洞、CloudBees Jenkins Job DSL Plugin 安全特征问题漏洞、

CloudBees Jenkins Credentials Plugin 信息泄露漏洞、CloudBees Jenkins PAM Authentication Plugin 信息泄露漏洞。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-2019-15063

http://www.cnvd.org.cn/flaw/show/CNVD-2019-15065

http://www.cnvd.org.cn/flaw/show/CNVD-2019-15074

http://www.cnvd.org.cn/flaw/show/CNVD-2019-15073

http://www.cnvd.org.cn/flaw/show/CNVD-2019-15076

http://www.cnvd.org.cn/flaw/show/CNVD-2019-15075

http://www.cnvd.org.cn/flaw/show/CNVD-2019-15112

http://www.cnvd.org.cn/flaw/show/CNVD-2019-15111

2、Oracle 产品安全漏洞

Oracle PeopleSoft Products 是一套企业人力资本管理解决方案。Oracle Supply Chain Products Suite 是一套供应链解决方案。Oracle Java SE 是一款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。Oracle Commerce 是一套电子商务解决方案。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞影响数据的保密性和完整性。

CNVD 收录的相关漏洞包括：Oracle PeopleSoft Products PeopleSoft Enterprise ELM 访问控制错误漏洞、Oracle Supply Chain Products Suite Configurator 访问控制错误漏洞、Oracle PeopleSoft Products PeopleSoft Enterprise HCM Talent Acquisition Manager 访问控制错误漏洞、Oracle PeopleSoft Products PeopleSoft Enterprise PT PeopleTools 信息泄露漏洞、Oracle PeopleSoft Products PeopleSoft Enterprise PT PeopleTools 访问控制错误漏洞、Oracle PeopleSoft Products PeopleSoft Enterprise HRMS 访问控制错误漏洞、Oracle Java SE 访问控制错误漏洞、Oracle Commerce Merchandising 组件访问控制错误漏洞。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-2019-14888

http://www.cnvd.org.cn/flaw/show/CNVD-2019-14887

http://www.cnvd.org.cn/flaw/show/CNVD-2019-14933

http://www.cnvd.org.cn/flaw/show/CNVD-2019-14932

http://www.cnvd.org.cn/flaw/show/CNVD-2019-14935

http://www.cnvd.org.cn/flaw/show/CNVD-2019-14934

http://www.cnvd.org.cn/flaw/show/CNVD-2019-14955

http://www.cnvd.org.cn/flaw/show/CNVD-2019-14956

3、Google 产品安全漏洞

Android 是美国谷歌（Google）和开放手持设备联盟（简称 OHA）的一套以 Linux 为基础的开源操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，执行任意代码等。

CNVD 收录的相关漏洞包括：Google Android Binder 驱动程序权限许可和访问控制漏洞、Google Android System 权限提升漏洞（CNVD-2019-15175、CNVD-2019-15188、CNVD-2019-15189、CNVD-2019-15194、CNVD-2019-15195、CNVD-2019-15196）、Google Android Media framework 权限提升漏洞（CNVD-2019-15201）。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-2019-15173
http://www.cnvd.org.cn/flaw/show/CNVD-2019-15175
http://www.cnvd.org.cn/flaw/show/CNVD-2019-15188
http://www.cnvd.org.cn/flaw/show/CNVD-2019-15189
http://www.cnvd.org.cn/flaw/show/CNVD-2019-15194
http://www.cnvd.org.cn/flaw/show/CNVD-2019-15195
http://www.cnvd.org.cn/flaw/show/CNVD-2019-15196
http://www.cnvd.org.cn/flaw/show/CNVD-2019-15201

4、GitLab 产品安全漏洞

GitLab 是一款使用 Ruby on Rails 开发的、自托管的、Git（版本控制系统）项目仓库应用程序。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，打开重定向，导致资源消耗等。

CNVD 收录的相关漏洞包括：GitLab 资源管理错误漏洞、GitLab 输入验证错误漏洞、GitLab 访问控制错误漏洞（CNVD-2019-14882、CNVD-2019-14949、CNVD-2019-14951、CNVD-2019-14950）、GitLab 信息泄露漏洞（CNVD-2019-14812、CNVD-2019-14952）。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-2019-14811
http://www.cnvd.org.cn/flaw/show/CNVD-2019-14813
http://www.cnvd.org.cn/flaw/show/CNVD-2019-14812
http://www.cnvd.org.cn/flaw/show/CNVD-2019-14882
http://www.cnvd.org.cn/flaw/show/CNVD-2019-14949
http://www.cnvd.org.cn/flaw/show/CNVD-2019-14951
http://www.cnvd.org.cn/flaw/show/CNVD-2019-14950
http://www.cnvd.org.cn/flaw/show/CNVD-2019-14952

5、ALE Alcatel OmniAccess Wireless Access Point 命令注入漏洞

ALE Alcatel OmniAccess Wireless Access Point 是一款无线接入点设备。

ALE Alcatel OmniAccess Wireless Access Point 被披露存在命令注入漏洞。攻击者可利用该漏洞执行非法命令。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-2019-15207

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-2019-14808	OpenEMR SQL 注入漏洞（CNVD-2019-14808）	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.open-emr.org/wiki/index.php/OpenEMR_Patches#5.0.1_Patch_.289.2F9.2F18.29
CNVD-2019-14819	Siemens SIMATIC PCS 7 和 SIMATIC WinCC 访问控制错误漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://cert-portal.siemens.com/productcert/pdf/ssa-705517.pdf
CNVD-2019-14847	Sysdig 安全绕过漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/falcosecurity/falco/pull/561
CNVD-2019-14930	PaperStream IP DLL 劫持漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.fujitsu.com/
CNVD-2019-14953	SimplyBook.me 远程代码执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://news.simplybook.me/notification/
CNVD-2019-15088	UltraVNC 缓冲区溢出漏洞（CNVD-2019-15088）	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://ics-cert.kaspersky.com/advisories/klcert-advisories/2019/03/01/klcert-19-007-ultravnc-out-of-bound-read/
CNVD-2019-15095	Samsung Galaxy S9 代码执行漏洞（CNVD-2019-15095）	高	目前厂商已发布新版本，以修复此安全问题，详情请关注厂商主页：https://www.samsung.com/
CNVD-2019-15102	Atlassian Sourcetree 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/SRCTREE-6391
CNVD-201	UltraVNC 越界访问漏洞	高	厂商已发布漏洞修复程序，请及时关

9-15210			注更新：https://www.uvnc.com/
CNVD-2019-15327	Koji 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://docs.pagure.org/koji/CVE-2018-1002161/

小结：本周，CloudBees 被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，绕过沙盒保护，执行任意代码等。此外，Oracle、Google、GitLab 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，打开重定向，提升权限，执行任意代码，导致资源消耗等。ALE Alcatel OmniAccess Wireless Access Point 被披露存在命令注入漏洞。攻击者可利用该漏洞执行非法命令。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、MacDown 远程代码执行漏洞

验证描述

MacDown 是一款适用于 macOS 平台的开源 Markdown 编辑器。

MacDown 0.7.1 (870)版本中存在远程代码执行漏洞，该漏洞源于程序未能对输入进行过滤，攻击者可利用该漏洞执行任意代码。

验证信息

POC 链接：https://github.com/MacDownApp/macdown/issues/1050

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-14834

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. 安全人员发现 macOS Gatekeeper 认证漏洞，可获取系统 shell

安全研究人员近日发现了在 macOS 10.14.5 上的一个安全的漏洞，可以忽略掉系统安全的第一个屏障 Gatekeeper 来直接运行不安全的应用，并且从而获得了系统的 Shell 权限。Gatekeeper 是 Mac App Store 的一个很关键的防御措施，当你的应用没有被安全签名，系统是无法运行这个应用的。这个漏洞可以让不太了解的用户，通过获取恶意邮

件等方式在不知情的情况下运行此应用而给系统带来一定的风险。但是获取 Shell 是需要系统打开 ssh 登录等后门。这个对于一般用户来说影响不大。因为一般用户不会激活共享设置里的远程访问功能。此问题已经提交给苹果。预计很快会进行修复。

参考链接：https://www.fcvl.net/vulnerabilities/macosx-gatekeeper-bypass

2. GitHub ID 为 SandboxEscaper 的用户再次上传 2 个零日漏洞

GitHub ID 为 SandboxEscaper 的用户之前在 GitHub 上上传了类似的安全功能漏洞之后，漏洞来自 Windows 错误报告功能以及 IE 11 模块。成功利用错误报告功能存在的漏洞可让黑客获得提权能力，编辑原先无法访问的文件。而 IE 11 的漏洞则能够让攻击者在 Internet Explorer 中注入恶意代码。

参考链接：https://www.zdnet.com/article/two-more-microsoft-zero-days-uploaded-on-github/

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