国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2020 年 01 月 13 日-2020 年 01 月 19 日　　2020 年第 3 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 354 个，其中高危漏洞 160 个、中危漏洞 176 个、低危漏洞 18 个。漏洞平均分值为 6.52。本周收录的漏洞中，涉及 0day 漏洞 187 个（占 53%），其中互联网上出现“D-Link DIR-615 跨站脚本漏洞（CNVD-2020-02707）、SpotOutlook 拒绝服务漏洞”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 2126 个，与上周（1994 个）环比增长 7%。

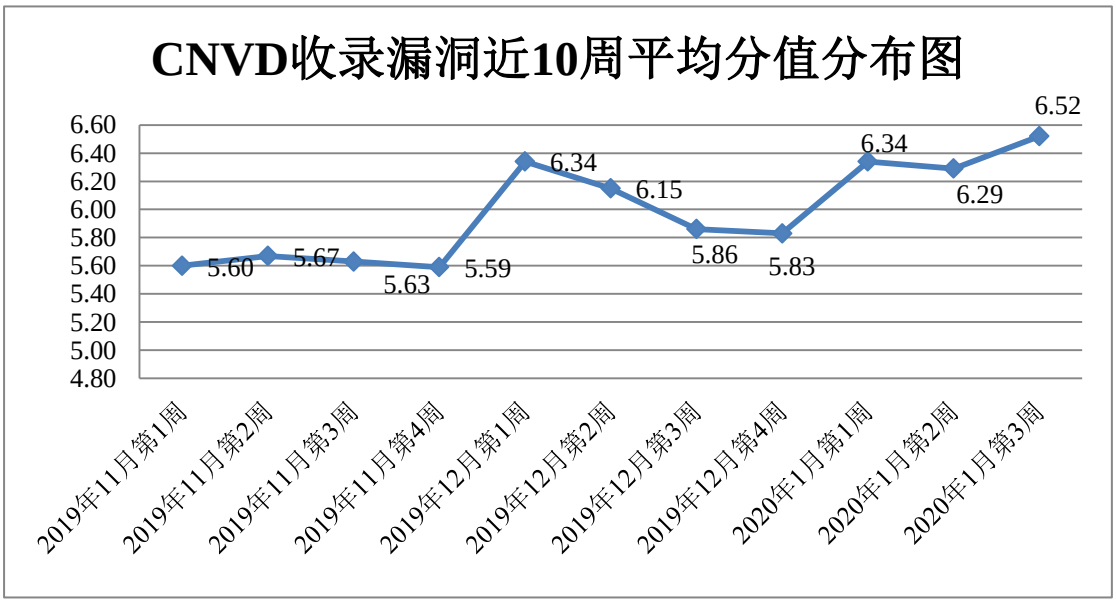

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞事件处置情况

本周，CNVD 向银行、保险、能源等重要行业单位通报漏洞事件 27 起，向基础电信企业通报漏洞事件 3 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 393 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 44 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 20 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：

北京百容千域软件技术开发有限责任公司、北京火绒网络科技有限公司、北京极地信息技术有限公司、北京江民新科技术有限公司、北京搜麦联网络科技有限公司、倍福自动化有限公司、成都飞鱼星科技股份有限公司、成都依能科技股份有限公司、成都职工投资集团有限公司、福州富昌维控电子科技有限公司、广州华多网络科技有限公司、广州联雅网络科技有限公司、广州凌科普华网络科技有限公司、广州粤建三和软件股份有限公司、国药集团医药物流有限公司、海南易而优科技有限公司、河南标点科技有限公司、江门市蓬江区科汇发展有限公司、江苏巡天网络科技有限公司、六安校无忧信息科技有限公司、洛阳云业信息科技有限公司、南昌掌易业泰科技有限公司、农信银资金清算中心有限责任公司、陕西亚皇科技有限公司、上海顶想信息科技有限公司、深圳华颐智能系统有限公司、深圳市乙辰科技股份有限公司、深圳微缘信息科技有限公司、深圳雅科网络科技有限公司、石家庄和嘉科技有限公司、石家庄九帆网络技术有限公司、四平市九州易通科技有限公司、苏州麦软网络有限公司、西安佰联网络技术有限公司、西安长臂猿网络有限公司、西安知先信息技术有限公司、义乌畅流网络科技有限公司、长沙德尚网络科技有限公司、长沙米拓信息技术有限公司、浙江禾匠信息科技有限公司、镇江市云优网络科技有限公司、中金金采网络技术（北京）有限公司、中铁八局集团有限公司、中铁十二局集团第四工程有限公司、中铁资源集团有限公司、中银金行有限公司、苦菊软件、荣茂网络、巡云网、乘风原创程序、中国建筑科学研究院、中国铁道学会、Angel 工作室网络网络科技有限公司、Catfish CMS、iCMS、MyuCMS、Pablo Software Solutions、PHPMywind、SparkPost 和 VideoLAN。

本周，CNVD 发布了《Microsoft 发布 2020 年 1 月安全更新》和《Oracle 发布 2020 年 1 月的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/5377

https://www.cnvd.org.cn/webinfo/show/5375

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，华为技术有限公司、北京天融信网络安全技术有限公司、哈尔滨安天科技集团股份有限公司、深信服科技股份有限公司、恒安嘉新(北京)科技股份公司等单位报送公开收集的漏洞数量较多。山东新潮信息技术有限公司、河南灵创电子科技有限公司、内蒙古洞明科技有限公司、远江盛邦（北京）网络安全科

技股份有限公司、南京众智维信息科技有限公司、北京华云安信息技术有限公司、山东云天安全技术有限公司、河南信安世纪科技有限公司、杭州迪普科技股份有限公司、国瑞数码零点实验室、内蒙古奥创科技有限公司、四川月安客信息技术有限公司、上海端御信息科技有限公司、长春嘉诚信息技术股份有限公司、四川雾都信息技术有限公司、厦门靠谱云股份有限公司、京东云安全、成都鹏博士电信传媒集团股份有限公司、广州万方计算机科技有限公司、山石网科通信技术股份有限公司及其他个人白帽子向 CNVD 提交了 2126 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）、斗象科技（漏洞盒子）和上海交大向 CNVD 共享的白帽子报送的 1212 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
斗象科技（漏洞盒子）	610	610
上海交大	317	317
奇安信网神（补天平台）	285	285
华为技术有限公司	253	0
北京天融信网络安全技术有限公司	129	1
哈尔滨安天科技集团股份有限公司	116	0
深信服科技股份有限公司	86	0
恒安嘉新(北京)科技股份公司	59	0
中国电信集团系统集成有限责任公司	57	57
北京启明星辰信息安全技术有限公司	55	0
北京神州绿盟科技有限公司	53	3
新华三技术有限公司	50	0
厦门服云信息科技有限公司	49	0
西安四叶草信息技术有限公司	33	33
北京数字观星科技有限公司	20	0
北京知道创宇信息技术股份有限公司	6	0

山东新潮信息技术有限公司	120	120
河南灵创电子科技有限公司	78	78
内蒙古洞明科技有限公司	75	75
远江盛邦（北京）网络安全科技股份有限公司	67	67
南京众智维信息科技有限公司	66	66
北京华云安信息技术有限公司	40	40
山东云天安全技术有限公司	16	16
河南信安世纪科技有限公司	13	13
杭州迪普科技股份有限公司	13	0
国瑞数码零点实验室	10	10
内蒙古奥创科技有限公司	8	8
四川月安客信息技术有限公司	4	4
上海端御信息科技有限公司	2	2
长春嘉诚信息技术股份有限公司	2	2
四川雾都信息技术有限公司	1	1
厦门靠谱云股份有限公司	1	1
京东云安全	1	1
成都鹏博士电信传媒集团股份有限公司	1	1
广州万方计算机科技有限公司	1	1
山石网科通信技术股份有限公司	1	1
CNCERT 宁夏分中心	15	15
CNCERT 甘肃分中心	11	11

CNCERT 河北分中心	6	6
CNCERT 海南分中心	4	4
CNCERT 重庆分中心	2	2
CNCERT 上海分中心	2	2
CNCERT 湖南分中心	2	2
CNCERT 吉林分中心	1	1
CNCERT 贵州分中心	1	1
个人	269	269
报送总计	3011	2126

本周漏洞按类型和厂商统计

本周，CNVD 收录了 354 个漏洞。应用程序 151 个，WEB 应用 107 个，网络设备（交换机、路由器等网络端设备）37 个，操作系统 25 个，安全产品 18 个，数据库 13 个，智能设备（物联网终端设备）漏洞 3 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	151
WEB 应用	107
网络设备（交换机、路由器等网络端设备）	37
操作系统	25
安全产品	18
数据库	13
智能设备（物联网终端设备）漏洞	3

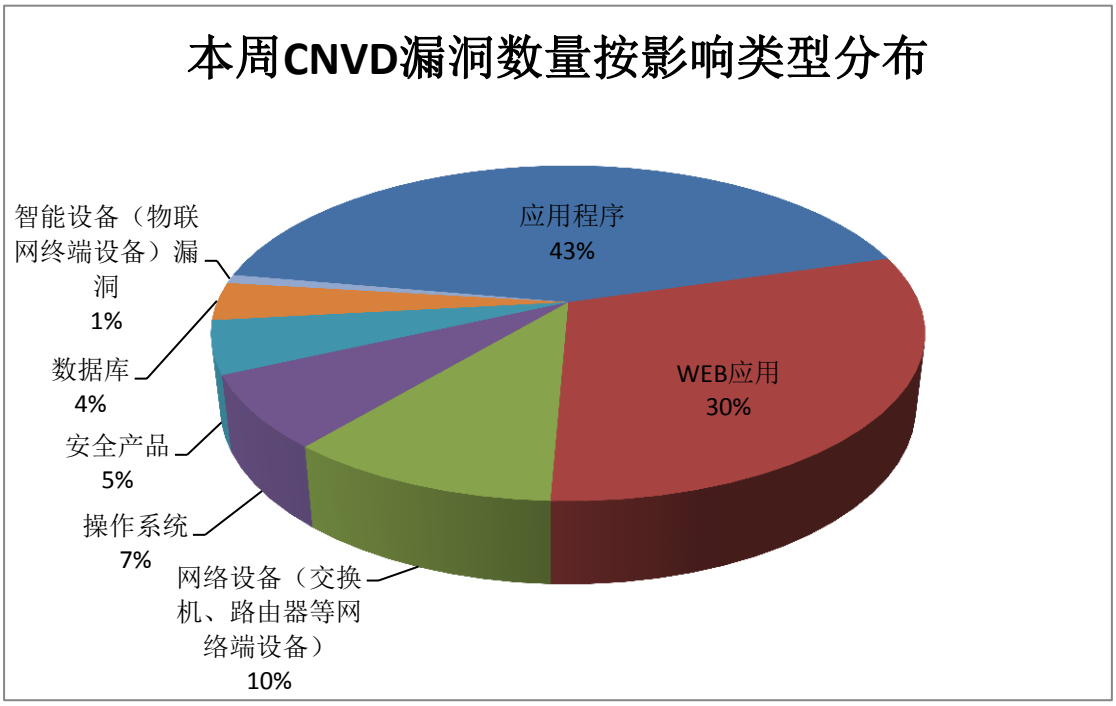

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Microsoft、Oracle、Red Hat 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	Microsoft	19	5%
2	Oracle	14	4%
3	Red Hat	14	4%
4	Apple	11	3%
5	iPubsoft Studio	9	3%
6	PostgreSQL	8	2%
7	Linux	6	2%
8	GitLab	6	2%
9	WordPress	6	2%
10	其他	261	73%

本周行业漏洞收录情况

本周，CNVD 收录了 24 个电信行业漏洞，19 个移动互联网行业漏洞，14 个工控行业漏洞（如下图所示）。其中，“PostgreSQL 缓冲区溢出漏洞、多款 Apple 产品 sysdiagnose 组件内存破坏漏洞、多款 Siemens 产品访问绕过漏洞、OSIsoft PI Vision 跨站请求

伪造漏洞”等漏洞的综合评级为“高危”。相关厂商已经发布了漏洞的修补程序，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/

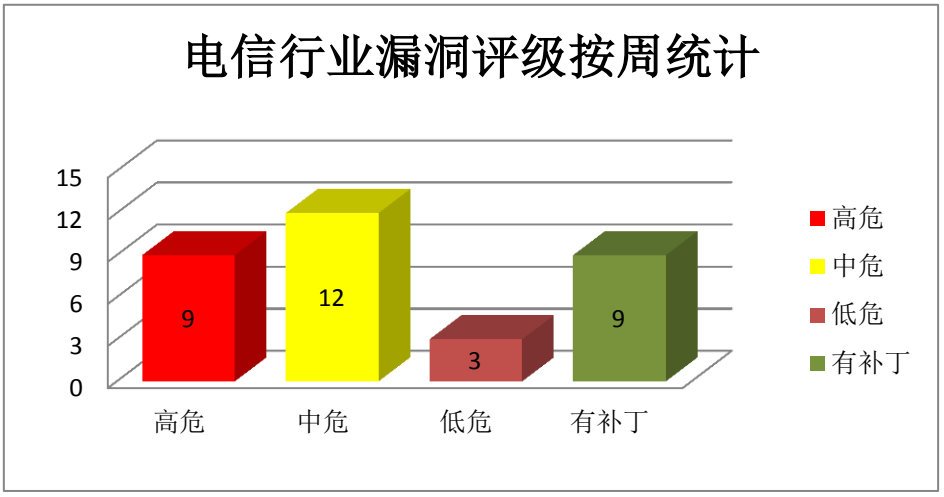

图 3 电信行业漏洞统计

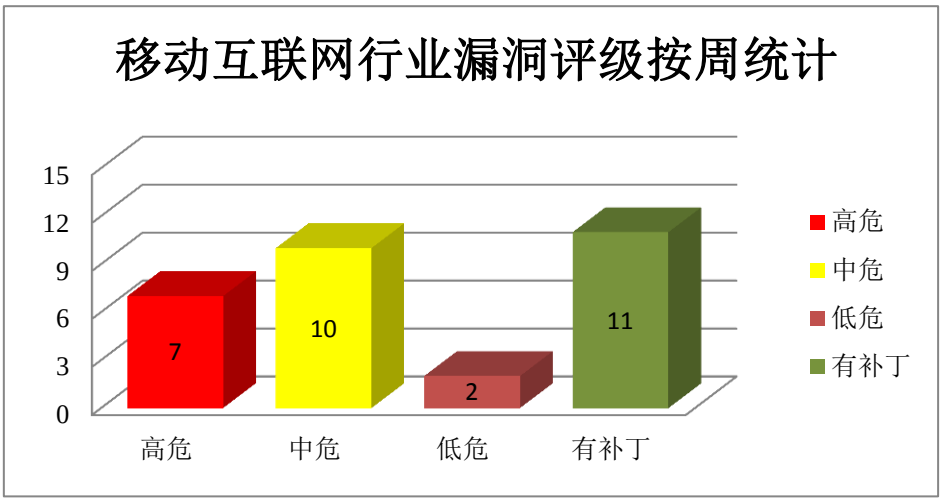

图 4 移动互联网行业漏洞统计

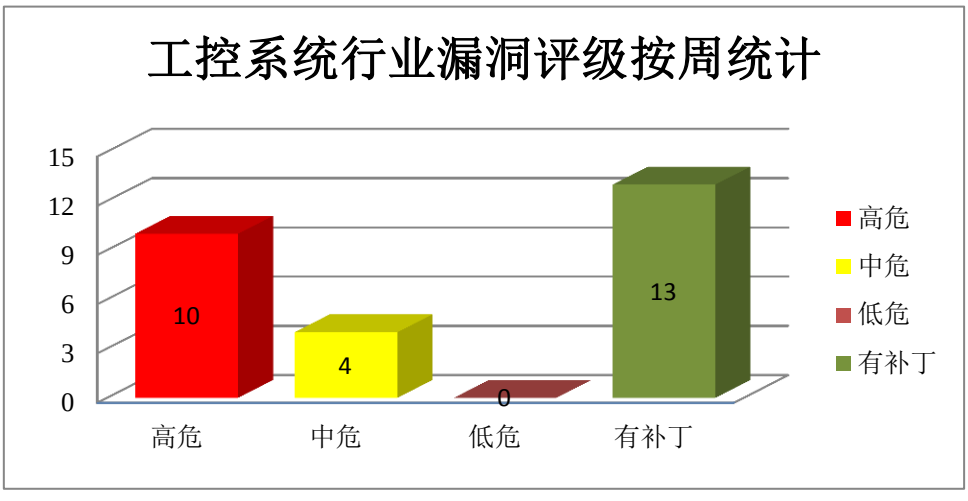

图 5 工控系统行业漏洞统计

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、Microsoft 产品安全漏洞

Microsoft Windows 和 Microsoft Windows Server 都是美国微软（Microsoft）公司的产品。Microsoft Windows 是一套个人设备使用的操作系统。Microsoft Windows Server 是一套服务器操作系统。Microsoft Office 是一款办公软件套件产品。Microsoft Word 是一套 Office 套件中的文字处理软件。Microsoft Internet Explorer（IE）是一款 Windows 操作系统附带的 Web 浏览器。Microsoft CryptoAPI 是微软提供给开发人员的 Windows 安全服务应用程序接口。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，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Microsoft Windows 和 Microsoft Windows Server 权限提升漏洞（CNVD-2020-02180、CNVD-2020-02182）、Microsoft Windows Kerne 权限提升漏洞、Microsoft PowerPoint 远程执行代码漏洞、Microsoft Word 拒绝服务漏洞、Microsoft Windows 和 Microsoft Windows Server 远程代码执行漏洞（CNVD-2020-02189）、Microsoft Internet Explorer 远程代码执行漏洞（CNVD-2020-02439）、Microsoft Windows CryptoAPI 欺骗漏洞。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-2020-02180

http://www.cnvd.org.cn/flaw/show/CNVD-2020-02182

http://www.cnvd.org.cn/flaw/show/CNVD-2020-02190

http://www.cnvd.org.cn/flaw/show/CNVD-2020-02187

http://www.cnvd.org.cn/flaw/show/CNVD-2020-02188

http://www.cnvd.org.cn/flaw/show/CNVD-2020-02189

http://www.cnvd.org.cn/flaw/show/CNVD-2020-02439

http://www.cnvd.org.cn/flaw/show/CNVD-2020-02446

2、Apple 产品安全漏洞

Apple iOS 等都是美国苹果（Apple）公司的产品。Apple iOS 是一套为移动设备所开发的操作系统。Apple tvOS 是一套智能电视操作系统。Apple watchOS 是一套智能手表操作系统。Apple Safari 是一款 Web 浏览器。Apple macOS Mojave 是一套专为 Mac 计算机所开发的专用操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过沙盒限制，获取 root 权限，执行任意代码等。

CNVD 收录的相关漏洞包括：多款 Apple 产品 sysdiagnose 组件内存破坏漏洞、Ap

ple iOS 和 Apple macOS Mojave Feedback Assistant 组件竞争条件漏洞、多款 Apple 产品 CoreAudio 组件越界读取漏洞、多款 Apple 产品 Kernel 组件越界读取漏洞、多款 Apple 产品 WebKit 组件内存破坏漏洞（CNVD-2020-01907、CNVD-2020-01929、CNVD-2020-01927、CNVD-2020-01930）。其中，“多款 Apple 产品 sysdiagnose 组件内存破坏漏洞、Apple iOS 和 Apple macOS Mojave Feedback Assistant 组件竞争条件漏洞、多款 Apple 产品 Kernel 组件越界读取漏洞”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-2020-01906
http://www.cnvd.org.cn/flaw/show/CNVD-2020-01907
http://www.cnvd.org.cn/flaw/show/CNVD-2020-01908
http://www.cnvd.org.cn/flaw/show/CNVD-2020-01926
http://www.cnvd.org.cn/flaw/show/CNVD-2020-01928
http://www.cnvd.org.cn/flaw/show/CNVD-2020-01929
http://www.cnvd.org.cn/flaw/show/CNVD-2020-01927
http://www.cnvd.org.cn/flaw/show/CNVD-2020-01930

3、Red Hat 产品安全漏洞

Red Hat Keycloak 是美国红帽（Red Hat）公司的一套为现代应用和服务提供身份验证和管理功能的软件。Red Hat OpenShift 是一款平台即服务（PaaS）云计算平台。Red Hat libvirt 是一个用于实现 Linux 虚拟化功能的 Linux API。Red Hat JBoss Enterprise Application Platform（EAP）是一套开源的、基于 J2EE 的中间件平台。Red Hat Enterprise Linux（RHEL）是一套面向企业用户的 Linux 操作系统。Red Hat JBoss BRMS 是一套用于开发容器化微服务和应用，以实现业务决策自动化的平台。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞向服务器发送非预期的请求，获取敏感信息，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Red Hat Keycloak 开放重定向漏洞、Red Hat OpenShift 跨站请求伪造漏洞、Red Hat libvirt 权限许可和访问控制问题漏洞、Red Hat libvirt 安全绕过漏洞、Red Hat JBoss Enterprise Application Platform 跨站脚本漏洞（CNVD-2020-01940）、Red Hat Enterprise Linux 资源管理错误漏洞、Red Hat JBoss BRMS 跨站脚本漏洞、Red Hat Keycloak 跨站脚本漏洞（CNVD-2020-01944）。其中，“Red Hat Enterprise Linux 资源管理错误漏洞”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-2020-01654
http://www.cnvd.org.cn/flaw/show/CNVD-2020-01921

http://www.cnvd.org.cn/flaw/show/CNVD-2020-01938

http://www.cnvd.org.cn/flaw/show/CNVD-2020-01939

http://www.cnvd.org.cn/flaw/show/CNVD-2020-01940

http://www.cnvd.org.cn/flaw/show/CNVD-2020-01941

http://www.cnvd.org.cn/flaw/show/CNVD-2020-01945

http://www.cnvd.org.cn/flaw/show/CNVD-2020-01944

4、Oracle 产品安全漏洞

Oracle Fusion Middleware（Oracle 融合中间件）是美国甲骨文（Oracle）公司的一套面向企业和云环境的业务创新平台。Oracle MySQL 是一套开源的关系数据库管理系统。Oracle E-Business Suite（电子商务套件）是一套全面集成式的全球业务管理软件。Oracle Sun Systems Products Suite 是一款 Sun 系统产品套件。本周，上述产品被披露存在访问控制错误漏洞，攻击者可利用漏洞未授权访问、更新、插入或删除数据。

CNVD 收录的相关漏洞包括：Oracle Fusion Middleware WebCenter Portal 访问控制错误漏洞（CNVD-2020-02562、CNVD-2020-02580）、Oracle Fusion Middleware HTTP Server 访问控制错误漏洞、Oracle Fusion Middleware Web Cache 访问控制错误漏洞、Oracle E-Business Suite Advanced Outbound Telephony 组件访问控制错误漏洞、Oracle Managed File Transfer 访问控制错误漏洞、Oracle Sun Systems Products Suite Sun ZFS Storage Appliance Kit 访问控制错误漏洞、Oracle MySQL Connectors 访问控制错误漏洞（CNVD-2020-02561）。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-2020-02562

http://www.cnvd.org.cn/flaw/show/CNVD-2020-02561

http://www.cnvd.org.cn/flaw/show/CNVD-2020-02560

http://www.cnvd.org.cn/flaw/show/CNVD-2020-02565

http://www.cnvd.org.cn/flaw/show/CNVD-2020-02564

http://www.cnvd.org.cn/flaw/show/CNVD-2020-02563

http://www.cnvd.org.cn/flaw/show/CNVD-2020-02566

http://www.cnvd.org.cn/flaw/show/CNVD-2020-02580

5、 D-Link DIR-601 认证绕过漏洞

D-Link DIR-601 B1 是中国台湾友讯（D-Link）公司的一款无线路由器。本周，D-Link DIR-601 被披露存在认证绕过漏洞。该漏洞源于程序仅在客户端而未能在服务器端进行身份验证。攻击者可利用该漏洞绕过身份验证，执行任意操作。目前，厂商尚未发布上述漏洞的修补程序。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-2020-02551

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-2020-01603	MetInfo 存在文件上传漏洞（CNVD-2020-01603）	高	厂商反馈，已发布了漏洞修复程序，请及时关注更新：https://www.mituo.cn/
CNVD-2020-01911	GitLab 路径遍历漏洞（CNVD-2020-01911）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://about.gitlab.com/blog/2019/11/27/security-release-gitlab-12-5-1-released/
CNVD-2020-01955	Git for Visual Studio 远程代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-1350
CNVD-2020-02149	Mozilla Firefox ESR 和 Mozilla Firefox 类型混淆漏洞	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.mozilla.org/en-US/security/advisories/mfsa2020-03/
CNVD-2020-02280	HisiPHP v2.0.10 后台存在文件上传漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://gitee.com/hisi/hisiphp/commit/7124352ef84c759d3202e9e2104016caaa7da1e2 https://gitee.com/hisi/hisiphp/commit/dbd5dbe07cce2c1ae5532f85ed6237469471bbbe
CNVD-2020-02465	D-Link DCS-960L 缓冲区溢出远程代码执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10142
CNVD-2020-02547	Micro Focus AcuToWeb 信息泄露漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://softwaresupport.softwaregrp.com/doc/KM03569662
CNVD-2020-02573	Apache Olingo 代码问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://mail-archives.apache.org/mod_mbox/olingo-user/201912.mbox/%3CCAGSZ4d4vbSYaVh3aUWAvcVHK2qcFx

			xCZd3WAx3xbwZXskPX8nw%40mail.gmail.com%3E
CNVD-2020-02572	Facebook HHVM 缓冲区溢出漏洞（CNVD-2020-02572）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/facebook/hhvm/commit/1c518555dba6ceb45d5ba61845b96e261219c3b7
CNVD-2020-02609	Eclipse Che 跨站请求伪造漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://bugs.eclipse.org/bugs/show_bug.cgi?id=551596

小结：本周，Microsoft 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，导致拒绝服务等。此外，Apple、Red Hat、Oracle 等多款产品被披露存在多个漏洞，攻击者可利用漏洞获取 root 权限，执行任意代码，导致拒绝服务等。另外，D-Link DIR-601 被披露存在认证绕过漏洞。攻击者可利用该漏洞绕过身份验证，执行任意操作。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、D-Link DIR-615 跨站脚本漏洞（CNVD-2020-02707）

验证描述

D-Link DIR-615 是中国台湾友讯（D-Link）公司的一款无线路由器。

D-Link DIR-615 中的用户账户配置页面存在跨站脚本漏洞。该漏洞源于 WEB 应用缺少对客户端数据的正确验证。攻击者可利用该漏洞执行客户端代码。

验证信息

POC 链接：https://www.exploit-db.com/exploits/47776

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-02707

信息提供者

新华三技术有限公司

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. “微软超级漏洞”？关于 CVE-2020-0601 的官方回复

在微软例行公布的 1 月补丁更新列表中，有一个漏洞引起了大家的高度关注：一个

位于 CryptoAPI.dll 椭圆曲线密码(ECC)证书的验证绕过漏洞——CVE-2020-0601。有意思的是，在微软发布公告后，美国国家安全局（NSA）也发布了关于 CVE-2020-0601 漏洞的预警通告。根据通告可以得知，这个漏洞是由 NSA 率先独立发现并汇报给微软的（微软在报告中对 NSA 致谢）。

参考链接：https://www.freebuf.com/vuls/225524.html

2. 微软发布公告称 IE 0day 漏洞已遭利用，且无补丁

1 月 17 日，微软发布安全公告(ADV200001)称，一个 IE 0day(CVE-2020-0674)已遭利用，而且暂无补丁，仅有应变措施和缓解措施。微软表示正在推出解决方案，将在后续发布。微软表示该 IE 0day 已遭在野利用，并且指出这些利用只发生在“有限的目标攻击中”，该 0day 并未遭大规模利用，而只是针对少量用户攻击的一部分。

参考链接：https://www.cnbeta.com/articles/tech/933977.htm

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