

北京师范大学网络信息安全通告

2020 年 10 月报告

北京师范大学信息网络中心

2020 年 11 月

目录

漏洞态势	1
1. 公开漏洞情况.....	1
1.1. 漏洞增长概况.....	1
1.2. 漏洞分布情况.....	2
1.2.1. 漏洞厂商分布	2
1.2.2. 漏洞产品分布	2
1.2.3. 漏洞类型分布	3
1.2.4. 漏洞危害等级分布	5
1.3. 漏洞修复情况.....	5
1.3.1. 整体修复情况	5
1.3.2. 厂商修复情况	6
1.4. 重要漏洞实例	6
1.4.1. 超危漏洞实例	6
1.4.2. 高危漏洞实例	11
2. 接报漏洞情况.....	21
3. 重大漏洞预警.....	24
3.1. Oracle WebLogic 多个安全漏洞的预警	24
3.2. Vmware ESXi 安全漏洞的预警	27

漏洞态势

一、公开漏洞情况

根据国家信息安全漏洞库（CNNVD）统计，2020 年 10 月份新增安全漏洞共 1473 个，从厂商分布来看，Oracle 公司产品的漏洞数量最多，共发布 158 个；从漏洞类型来看，跨站脚本类的漏洞占比最大，达到 8.89%。本月新增漏洞中，超危漏洞 182 个、高危漏洞 612 个、中危漏洞 632 个、低危漏洞 47 个，相应修复率分别为 90.11%、92.16%、87.82%以及 95.74%。合计 1328 个漏洞已有修复补丁发布，本月整体修复率 90.16%。

截至 2020 年 10 月 31 日，CNNVD 采集漏洞总量已达 152892 个。

1.1 漏洞增长概况

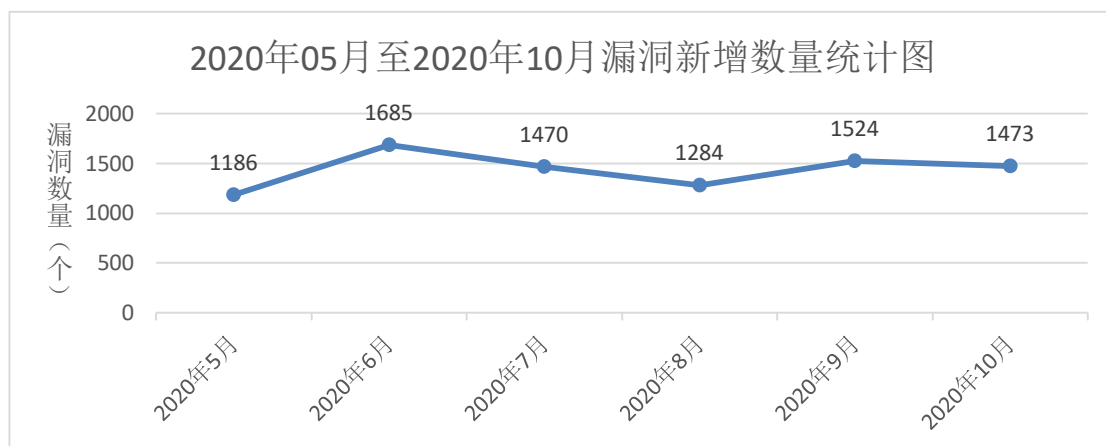


图 1 2020 年 5 月至 2020 年 10 月漏洞新增数量统计图

2020 年 10 月新增安全漏洞 1473 个，与上月（1524 个）相比减少了 3.35%。根据近 6 个月来漏洞新增数量统计图，平均每月漏洞数量达到 1437 个。

1.2 漏洞分布情况

1.2.1 漏洞厂商分布

10 月厂商漏洞数量分布情况如表 1 所示，Oracle 公司漏洞达到 158 个，占本月漏洞总量的 10.73%。

表 1 2020 年 10 月排名前十厂商新增安全漏洞统计表

序号	厂商名称	漏洞数量	所占比例
1	Oracle	158	10.73%
2	Apple	96	6.52%
3	Microsoft	91	6.18%
4	Google	67	4.55%
5	Cisco	56	3.80%
6	IBM	53	3.60%
7	NETGEAR	35	2.38%
8	Adobe	33	2.24%
9	Juniper Networks	31	2.10%
10	HP	27	1.83%

1.2.2 漏洞产品分布

10 月主流操作系统的漏洞统计情况如表 2 所示。本月 Windows 系列操作系统漏洞数量共 56 个。其中 Windows 10 漏洞数量最多，共 53 个，占主流操作系统漏洞总量的 16.99%，排名第一。

表 2 2020 年 10 月主流操作系统漏洞数量统计

序号	操作系统名称	漏洞数量
1	Windows 10	53
2	Windows Server 2019	46
3	Windows Server 2016	38

4	Android	27
5	Windows Server 2008	23
6	Windows Server 2008 R2	23
7	Windows 7	23
8	Windows Server 2012	20
9	Windows Server 2012 R2	20
10	Windows 8.1	19
11	Windows Rt 8.1	18
12	Linux Kernel	2

1.2.3 漏洞类型分布

10 月份发布的漏洞类型分布如表 3 所示，其中跨站脚本类漏洞所占比例最大，约为 8.89%。

表 3 2020 年 10 月漏洞类型统计表

序号	漏洞类型	漏洞数量（个）	所占比例
1	跨站脚本	131	8.89%
2	缓冲区错误	125	8.49%
3	输入验证错误	73	4.96%
4	代码问题	65	4.41%
5	授权问题	62	4.21%
6	信息泄露	57	3.87%
7	资源管理错误	46	3.12%
8	访问控制错误	31	2.10%
9	路径遍历	27	1.83%
10	SQL 注入	24	1.63%
11	命令注入	22	1.49%
12	跨站请求伪造	21	1.43%
13	注入	17	1.15%
14	操作系统命令注入	16	1.09%
15	加密问题	12	0.81%
16	代码注入	10	0.68%
17	信任管理问题	10	0.68%
18	日志信息泄露	8	0.54%
19	竞争条件问题	6	0.41%
20	数据伪造问题	6	0.41%
21	安全特征问题	5	0.34%
22	后置链接	4	0.27%
23	权限许可和访问控制问题	3	0.20%

24	数字错误	3	0.20%
25	格式化字符串错误	1	0.07%
26	其他	688	46.71%

1.2.4 漏洞危害等级分布

根据漏洞的影响范围、利用方式、攻击后果等情况，从高到低可将其分为四个危害等级，即超危、高危、中危和低危级别。10月漏洞危害等级分布如图2所示，其中超危漏洞182条，占本月漏洞总数的12.36%。

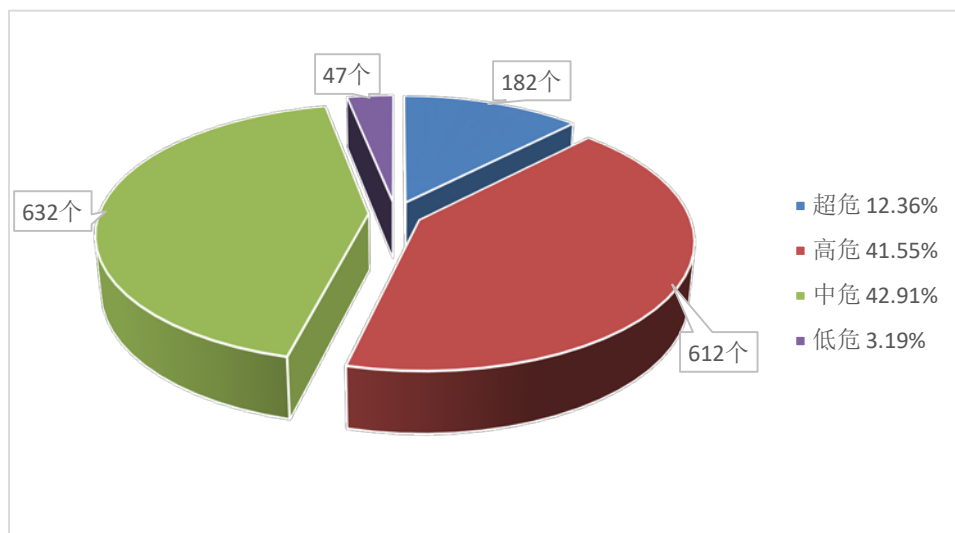


图2 2020年10月漏洞危害等级分布

1.3 漏洞修复情况

1.3.1 整体修复情况

10月漏洞修复情况按危害等级进行统计见图3。其中低危漏洞修复率最高，达到95.74%，中危漏洞修复率最低，比例为87.82%。总体来看，本月整体修复率，由上月的88.98%上升至本月的90.16%。

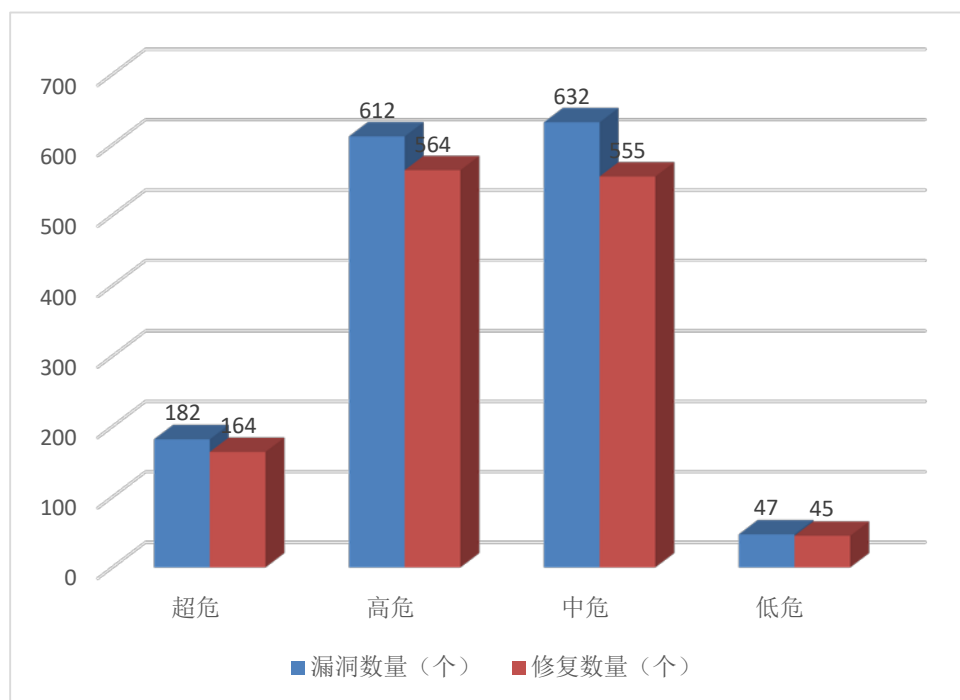


图3 2020年10月漏洞修复数量统计

1.3.2 厂商修复情况

10月漏洞修复情况按漏洞数量前十厂商进行统计,其中 Oracle、Apple、Microsoft 等十个厂商共 647 条漏洞,占本月漏洞总数的 43.92%,漏洞修复率为 97.53%,详细情况见表 4。多数知名厂商对产品安全高度重视,产品漏洞修复比较及时,其中 Oracle、Apple、Cisco、IBM、NETGEAR、Adobe、Juniper Networks、HP 等公司本月漏洞修复率均为 100%,共 631 条漏洞已全部修复。

表4 2020年10月厂商修复情况统计表

序号	厂商名称	漏洞数量 (个)	修复数量	修复率
1	Oracle	158	158	100.00%
2	Apple	96	96	100.00%
3	Microsoft	91	89	97.80%
4	Google	67	53	79.10%
5	Cisco	56	56	100.00%
6	IBM	53	53	100.00%
7	NETGEAR	35	35	100.00%
8	Adobe	33	33	100.00%

9	Juniper Networks	31	31	100.00%
10	HP	27	27	100.00%

1.4 重要漏洞实例

1.4.1 超危漏洞实例

本月超危漏洞共 182 个，其中重要漏洞实例如表 5 所示。

表 5 2020 年 10 月超危漏洞实例

序号	漏洞类型	CNNVD 编号	厂商	漏洞实例
1	SQL 注入	CNNVD-202010-719	Aptean	WordPress Loginizer SQL 注入漏洞 （CNNVD-202010-1186）
		CNNVD-202010-045	Artica	
		CNNVD-202010-088	Damstra	
		CNNVD-202010-007	WebsiteBaker	
		CNNVD-202010-1186	WordPress 基金会	
		CNNVD-202010-012	ZOHO	
		CNNVD-202010-1630		
		CNNVD-202010-383	phpMyAdmin 团队	
		CNNVD-202010-1623	个人开发者	
2	代码问题	CNNVD-202010-437	ARC Informatique	ARC Informatique PcVue 代码问题漏洞 （CNNVD-202010-437）
		CNNVD-202010-743	EclecticlQ	
		CNNVD-202010-823	Hewlett Packard Enterprise	
		CNNVD-202010-1580	SourceCodester	
		CNNVD-202010-387	个人开发者	
		CNNVD-202010-085		
		CNNVD-202010-1402	西安众邦网络	
3	授权问题	CNNVD-202010-1450	Aruba Networks	多款 NETGEAR 产品授权问题漏洞 （CNNVD-202010-358）
		CNNVD-202010-1139	Auth0	
		CNNVD-202010-815	Hewlett Packard Enterprise	
		CNNVD-202010-031	IBM	
		CNNVD-202010-1443	Konzept-iX	
		CNNVD-202010-360	NETGEAR	
		CNNVD-202010-359		
		CNNVD-202010-358		
		CNNVD-202010-126	RocketLinx	
		CNNVD-202010-057	WAVLINK	

		CNNVD-202010-257	yworks	
		CNNVD-202010-1085	个人开发者	
		CNNVD-202010-240		
4	操作系统命令注入	CNNVD-202010-465	SAP	SAP 操作系统命令注入漏洞（CNNVD-202010-465）
		CNNVD-202010-052	WAVLINK	
		CNNVD-202010-1429	个人开发者	
		CNNVD-202010-1424		
		CNNVD-202010-1582		
5	缓冲区错误	CNNVD-202010-1512	Apple	Foxit Reader， PhantomPDF 缓冲区错误漏洞 （CNNVD-202010-048）
		CNNVD-202010-151	Facebook	
		CNNVD-202010-058	Foxit	
		CNNVD-202010-048		
		CNNVD-202010-819	GoPro	
		CNNVD-202010-281	Google	
		CNNVD-202010-280		
		CNNVD-202010-272		
		CNNVD-202010-273		
		CNNVD-202010-274	HPE	
		CNNVD-202010-817		
		CNNVD-202010-416		
		CNNVD-202010-1488	Western Digital	
		CNNVD-202010-725	个人开发者	
		CNNVD-202010-715		
		CNNVD-202010-137		
		CNNVD-202010-1449		
6	访问控制错误	CNNVD-202010-657	Adobe	Microsoft Azure 访问控制错误漏洞 （CNNVD-202010-546）
		CNNVD-202010-092	Damstra	
		CNNVD-202010-546	Microsoft	
		CNNVD-202010-1654	Synology	
7	资源管理错误	CNNVD-202010-050	Foxit	VMware ESXi 资源管理错误漏洞 （CNNVD-202010-966）
		CNNVD-202010-046		
		CNNVD-202010-966	VMware	
		CNNVD-202010-061	个人开发者	
8	输入验证错误	CNNVD-202010-1233	Apple	多款 Apple 产品输入验证错误漏洞 （CNNVD-202010-1483）
		CNNVD-202010-1483		
		CNNVD-202010-824	Hewlett Packard Enterprise	
		CNNVD-202010-818		
		CNNVD-202010-1490	Western Digital	
		CNNVD-202010-1485		
		CNNVD-202010-1224	microchip	
		CNNVD-202010-571	开源机器人基金会	

1. WordPress Loginizer SQL 注入漏洞（CNNVD-202010-1186）

WordPress 是 WordPress 基金会的一套使用 PHP 语言开发的博客平台。该平台支持在 PHP 和 MySQL 的服务器上架设个人博客网站。

WordPress Loginizer 1.6.4 之前版本存在 SQL 注入漏洞，该漏洞源于与 loginizer_login_failed 和 lz_valid_ip 过滤不严格导致。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

<https://plugins.trac.wordpress.org/changeset/2401010/loginizer>

2. ARC Informatique PcVue 代码问题漏洞（CNNVD-202010-437）

Pcvue 是法国彩虹（ARC Informatique）一款多功能 HMI-SCADA 软件，是可以监测客户资产的各个方面的一体化方案。PcVue 被广泛应用于工业控制，楼宇管理，能源管理，智能电网，能源分布，变电站自动化，安防/消防系统，公用设施，物料搬运，交通运输，可再生能源和基础设施等领域。

PcVue 8.10 版本及之后版本存在安全漏洞，该漏洞源于存在一个远程代码执行漏洞，这是由于在接口上接收到的消息不安全的反序列化。

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.pcvuesolutions.com/index.php/support-a-services/resources/security-alerts-95138>

3. 多款 NETGEAR 产品授权问题漏洞（CNNVD-202010-358）

NETGEAR RBK752 等都是美国网件（NETGEAR）公司的产品。NETGEAR RBK752 是一套家庭 WiFi 系统。RBR750 是一套家庭 WiFi

系统。NETGEAR RBK852 是一款路由器。

Certain NETGEAR devices CBR40 2.5.0.10 之前版本, RBK752 3.2.15.25 之前版本, RBR750 3.2.15.25 之前版本, RBS750 3.2.15.25 之前版本, RBK852 3.2.10.11 之前版本, RBR850 3.2.10.11 之前版本, RBS850 3.2.10.11 之前版本存在安全漏洞, 该漏洞允许攻击者进行身份验证绕过。

目前厂商已发布升级补丁以修复漏洞, 补丁获取链接:

<https://kb.netgear.com/000062326/Security-Advisory-for-Authentication-Bypass-on-Some-WiFi-Systems-PSV-2020-0028>

4. SAP 操作系统命令注入漏洞 (CNNVD-202010-465)

SAP Solution Manager 和 SAP Focused Run 都是德国思爱普(SAP)公司的产品。SAP Solution Manager 是一套集系统监控。SAP Focused Run 是一个数据中心和大客户系统运维管理方案。

SAP 存在安全漏洞, 远程攻击者通过构造特制的数据包, 发送到受影响的主机, 可造成远程命令执行。

目前厂商已发布升级补丁以修复漏洞, 补丁获取链接:

<https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=558632196>

5. Foxit Reader , PhantomPDF 缓冲区错误漏洞 (CNNVD-202010-048)

Reader 是一套 PDF 文档阅读软件。Foxit Reader 是一款 PDF 文档阅读器。V8 是其中的一个开源 JavaScript 引擎。mPDF 是一款使用

PHP 编写的用于将 HTML 转换成 PDF 文件的库。

Foxit Reader and PhantomPDF 10.1 之前版本存在缓冲区错误漏洞。该漏洞源于网络系统或产品在内存上执行操作时，未正确验证数据边界，导致向关联的其他内存位置上执行了错误的读写操作。攻击者可利用该漏洞导致缓冲区溢出或堆溢出等。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

<https://www.foxitsoftware.com/support/security-bulletins.html>

6. Microsoft Azure 访问控制错误漏洞（CNNVD-202010-546）

Microsoft Azure 是美国微软（Microsoft）公司的一套开放的企业级云计算平台。

Azure 存在安全漏洞，该漏洞源于 Azure 功能验证访问密钥的方式中存在特权提升漏洞。攻击者可利用该漏洞可以在没有正确授权的情况下调用 HTTP 功能。以下产品及版本受到影响：Azure Functions 版本。

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://azure.microsoft.com/en-au/services/functions/>

7. VMware ESXi 资源管理错误漏洞（CNNVD-202010-966）

VMware ESXi 是美国威睿（VMware）公司的一套可直接安装在物理服务器上的服务器虚拟化平台。

VMware ESXi 存在安全漏洞，该漏洞源于攻击者可以访问 ESXi 机器上的 427 端口，从而利用该漏洞导致远程代码执行。以下产品及版本受到影响：ESXi_7.0.1-0.0.16850804 7.0 之前版本，

ESXi670-202010401-SG 6.7 之前版本, ESXi650-202010401-SG 6.5 之前版本。

目前厂商已发布升级补丁以修复漏洞, 补丁获取链接:

<https://www.vmware.com/security/advisories/VMSA-2020-0023.html>

8. 多款 Apple 产品输入验证错误漏洞 (CNNVD-202010-1483)

Apple macOS Mojave 和 Apple watchOS 都是美国苹果 (Apple) 公司的产品。Apple macOS Mojave 是一套专为 Mac 计算机所开发的专用操作系统。Apple watchOS 是一套智能手表操作系统。

Apple 多款产品存在输入验证错误漏洞, 该漏洞源于未对输入的数据进行正确的验证。以下产品及版本受到影响: Apple watchOS 5.2 之前版本, Apple macOS Mojave 10.14.4 之前版本, Apple iOS 12.2 之前版本。

目前厂商已发布升级补丁以修复漏洞, 补丁获取链接:

<https://support.apple.com/en-us/HT209602>

1.4.2 高危漏洞实例

本月高危漏洞共 612 个, 其中重点漏洞实例如表 6 所示。

表 6 2020 年 10 月高危漏洞实例

序号	漏洞类型	CNNVD 编号	厂商	漏洞实例
1	SQL 注入	CNNVD-202010-697	Advantech	IBM Sterling BB Integrator SQL 注入漏洞 (CNNVD-202010-900)
		CNNVD-202010-446	I-net software	
		CNNVD-202010-900	IBM	
		CNNVD-202010-1681	Pimcore	
		CNNVD-202010-637	Rapid7	
		CNNVD-202010-1092	TIBCO Software	

		CNNVD-202010-1535	Victor Alagwu	
		CNNVD-202010-1137	WordPress 基金会	
		CNNVD-202010-162	ZOHO	
		CNNVD-202010-160		
		CNNVD-202010-209	个人开发者	
2	代码问题	CNNVD-202010-1119	Adobe	Microsoft Windows 图形设备接口 (GDI) 代码问题漏洞 (CNNVD-202010-519)
		CNNVD-202010-1110		
		CNNVD-202010-477		
		CNNVD-202010-1113		
		CNNVD-202010-1090		
		CNNVD-202010-1108		
		CNNVD-202010-1105	Adobe	
		CNNVD-202010-384	Apache	
		CNNVD-202010-1537	Check Point	
		CNNVD-202010-1147	Cisco	
		CNNVD-202010-233		
		CNNVD-202010-377	IBM	
		CNNVD-202010-1677		
		CNNVD-202010-224		
		CNNVD-202010-880	JetBrains	
		CNNVD-202010-577	Lenovo	
		CNNVD-202010-569		
		CNNVD-202010-1682	Linux 基金会	
		CNNVD-202010-196	McAfee	
		CNNVD-202010-263	Micro Star	
		CNNVD-202010-488	Microsoft	
		CNNVD-202010-519		
		CNNVD-202010-1404	NVIDIA	
		CNNVD-202010-111	PHPGroup	
		CNNVD-202010-1546	Pulse Secure	
		CNNVD-202010-1566		
		CNNVD-202010-691	Qualcomm	
		CNNVD-202010-432	Samsung	
		CNNVD-202010-1578	SonicWall	
		CNNVD-202010-1576		
		CNNVD-202010-1088	WECON Technologies	
		CNNVD-202010-1676	baserCMS	
CNNVD-202010-1055	个人开发者			
CNNVD-202010-1120				
CNNVD-202010-889				
CNNVD-202010-141				
CNNVD-202010-386				

		CNNVD-202010-1600		
3	授权问题	CNNVD-202010-724	Apereo	Apple OS X 授权问题漏洞 （CNNVD-202010-1236）
		CNNVD-202010-1247	Apple	
		CNNVD-202010-1236		
		CNNVD-202010-1239		
		CNNVD-202010-1440	Aruba Networks	
		CNNVD-202010-1150	Cisco	
		CNNVD-202010-107	ClickStudios	
		CNNVD-202010-324	ConnectWise	
		CNNVD-202010-376	IBM	
		CNNVD-202010-219	Johnson Controls	
		CNNVD-202010-739	Juniper Networks	
		CNNVD-202010-553	Lenovo	
		CNNVD-202010-500	Microsoft	
		CNNVD-202010-515		
		CNNVD-202010-499		
		CNNVD-202010-496		
		CNNVD-202010-517		
		CNNVD-202010-518		
		CNNVD-202010-503		
		CNNVD-202010-522		
		CNNVD-202010-490		
		CNNVD-202010-511		
		CNNVD-202010-513		
		CNNVD-202010-497		
		CNNVD-202010-1454	OpenSSL 团队	
		CNNVD-202010-1031	Oracle	
		CNNVD-202010-1040		
		CNNVD-202010-1043		
		CNNVD-202010-1684	VMware	
		CNNVD-202010-262	ZOHO	
		CNNVD-202010-809	mintegral	
4	操作系统 命令注入	CNNVD-202010-1152	Cisco	Cisco FXOS Software 操 作系统命令注入漏洞 （CNNVD-202010-1152）
		CNNVD-202010-720	Gogs	
		CNNVD-202010-579	Microhard	
		CNNVD-202010-1115	Nagios	
		CNNVD-202010-807	个人开发者	
		CNNVD-202010-1626		
		CNNVD-202010-726		
5	缓冲区错 误	CNNVD-202010-1087	Adobe	Red Hat SPICE remote display system 缓冲区错 误漏洞 （CNNVD-202010-194）
		CNNVD-202010-1098		
		CNNVD-202010-1079		
		CNNVD-202010-1077		

		CNNVD-202010-1100	
		CNNVD-202010-1094	
		CNNVD-202010-1083	
		CNNVD-202010-1072	
		CNNVD-202010-1107	
		CNNVD-202010-1078	
		CNNVD-202010-1074	
		CNNVD-202010-707	Amazon
		CNNVD-202010-812	AppNeta
		CNNVD-202010-811	
		CNNVD-202010-1209	Apple
		CNNVD-202010-1218	
		CNNVD-202010-1238	
		CNNVD-202010-1493	
		CNNVD-202010-1222	
		CNNVD-202010-1242	
		CNNVD-202010-1216	
		CNNVD-202010-1213	
		CNNVD-202010-1219	
		CNNVD-202010-1217	
		CNNVD-202010-1215	
		CNNVD-202010-1220	
		CNNVD-202010-1243	
		CNNVD-202010-1205	
		CNNVD-202010-1473	
		CNNVD-202010-1244	
		CNNVD-202010-1465	
		CNNVD-202010-1491	
		CNNVD-202010-1462	
		CNNVD-202010-1471	
		CNNVD-202010-1495	
		CNNVD-202010-1234	
		CNNVD-202010-1492	
		CNNVD-202010-1398	Belkin
		CNNVD-202010-068	Bitdefender
		CNNVD-202010-004	
		CNNVD-202010-239	Cisco
		CNNVD-202010-1168	
		CNNVD-202010-1453	Facebook
		CNNVD-202010-149	
		CNNVD-202010-595	Foxit
		CNNVD-202010-591	
		CNNVD-202010-590	

		CNNVD-202010-820	GoPro	
		CNNVD-202010-1184	Google	
		CNNVD-202010-1455		
		CNNVD-202010-1185		
		CNNVD-202010-285		
		CNNVD-202010-283		
		CNNVD-202010-640	Huawei	
		CNNVD-202010-1543	IBM	
		CNNVD-202010-222		
		CNNVD-202010-665	Juniper Networks	
		CNNVD-202010-578	LCDS	
		CNNVD-202010-699	Microsoft	
		CNNVD-202010-530		
		CNNVD-202010-492		
		CNNVD-202010-561		
		CNNVD-202010-484		
		CNNVD-202010-501		
		CNNVD-202010-504		
		CNNVD-202010-574		
		CNNVD-202010-556		
		CNNVD-202010-550		
		CNNVD-202010-516		
		CNNVD-202010-508		
		CNNVD-202010-1426	Motion-Projec	
		CNNVD-202010-093	NVIDIA	
		CNNVD-202010-194	Red Hat	
		CNNVD-202010-456	SAP	
		CNNVD-202010-455		
		CNNVD-202010-458		
		CNNVD-202010-413	SUSE	
		CNNVD-202010-419	SonicWall	
		CNNVD-202010-423		
		CNNVD-202010-421		
		CNNVD-202010-1192	fastdlabs	
		CNNVD-202010-135	个人开发者	
		CNNVD-202010-638		
		CNNVD-202010-706		
		CNNVD-202010-1270	英国剑桥大学	
6	访问控制 错误	CNNVD-202010-448	Acronis	Microsoft SharePoint 访问 控制错误漏洞 （CNNVD-202010-478）
		CNNVD-202010-450		
		CNNVD-202010-451	Adobe	
		CNNVD-202010-1140	Apache	
		CNNVD-202010-025		

		CNNVD-202010-542		
		CNNVD-202010-481	Microsoft	
		CNNVD-202010-478		
		CNNVD-202010-108	Nextcloud	
		CNNVD-202010-995		
		CNNVD-202010-1036	Oracle	
7	资源管理 错误	CNNVD-202010-1103	Adobe	
		CNNVD-202010-1518	Apple	
		CNNVD-202010-1146		
		CNNVD-202010-1163		
		CNNVD-202010-1154		
		CNNVD-202010-1173		
		CNNVD-202010-1161		
		CNNVD-202010-1158		
		CNNVD-202010-1157		
		CNNVD-202010-1169		
		CNNVD-202010-585		
		CNNVD-202010-598	Foxit	
		CNNVD-202010-1457		
		CNNVD-202010-1458		
		CNNVD-202010-1456	Google	
		CNNVD-202010-688		
		CNNVD-202010-686	Juniper Networks	
		CNNVD-202010-565	Microsoft	
		CNNVD-202010-098		
		CNNVD-202010-094	NVIDIA	
		CNNVD-202010-134	OpenSSL	
		CNNVD-202010-1562	Shibboleth	
		CNNVD-202010-646	个人开发者	
8	输入验证 错误	CNNVD-202010-1510		
		CNNVD-202010-1504		
		CNNVD-202010-1501		
		CNNVD-202010-1517		
		CNNVD-202010-1448	Chai.js 团队	
		CNNVD-202010-1144		
		CNNVD-202010-1171		
		CNNVD-202010-1174		
		CNNVD-202010-1143		
		CNNVD-202010-310		
		CNNVD-202010-278		
		CNNVD-202010-157	Google, LG	
		CNNVD-202010-679		
		CNNVD-202010-673	Juniper Networks	
				Google Chrome 资源管理 错误漏洞 (CNNVD-202010-1458)
				Linux kernel 输入验证错 误漏洞 (CNNVD-202010-133)

		CNNVD-202010-741		
		CNNVD-202010-661		
		CNNVD-202010-740		
		CNNVD-202010-666		
		CNNVD-202010-133	Linux 基金会	
		CNNVD-202010-534	Microsoft	
		CNNVD-202010-483		
		CNNVD-202010-555		
		CNNVD-202010-526		
		CNNVD-202010-537		
		CNNVD-202010-216	MikroTik	
		CNNVD-202010-095	NVIDIA	
		CNNVD-202010-312	Qualcomm	
		CNNVD-202010-123	RocketLinx	
		CNNVD-202010-142	Sierra Wireless	
		CNNVD-202010-1475	Texas	
		CNNVD-202010-1476	Instruments	
		CNNVD-202010-200	WordPress 基金会	
		CNNVD-202010-087	ZOHO	
		CNNVD-202010-892	个人开发者	
		CNNVD-202010-153		
		CNNVD-202010-152		
		CNNVD-202010-067		
		CNNVD-202010-728		
		CNNVD-202010-065		
		CNNVD-202010-714		

1. IBM Sterling BB Integrator SQL 注入漏洞(CNNVD-202010-900)

IBM Sterling B2B Integrator 是美国 IBM 公司的一套集成了重要的 B2B 流程、交易和关系的软件。该软件支持与不同的合作伙伴社区之间实现复杂的 B2B 流程的安全集成。

IBM Sterling B2B Integrator 存在 SQL 注入漏洞，该漏洞源于 Graphic Process Modeler 过滤不严格导致。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

<https://www.ibm.com/support/pages/node/6349515>

2. Microsoft Windows 图形设备接口 (GDI) 代码问题漏洞

(CNNVD-202010-519)

Microsoft Windows 是美国微软（Microsoft）公司的一种桌面操作系统。

Windows 图形设备接口 (GDI)存在代码问题漏洞。该漏洞允许攻击者控制受影响的系统。以下产品及版本受到影响： Windows 10 1909 版本， Windows 10 1709 版本， Windows Server 1909 版本， Windows Server 2004 版本， Windows Server 1903 版本， Windows 10 2004 版本， Windows 10 1809 版本， Windows RT 8.1 版本， Windows 8.1 版本， Windows Server 2016 版本， Windows Server 2012 版本， Windows 10 版本， Windows Server 2012 R2 版本， Windows 10 1803 版本， Windows 10 1903 版本， Windows Server 2019 版本， Windows 10 1607 版本。

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://portal.msrc.microsoft.com/en-us/security-guidance>

3. Apple OS X 授权问题漏洞 (CNNVD-202010-1236)

Apple OS X 是美国苹果（Apple）公司的一套为 Mac 计算机所开发的专用操作系统。

OS XIntel Graphics Driver 存在授权问题漏洞，该漏洞使恶意应用程序能够以系统特权执行任意代码。

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://support.apple.com/>

4. Cisco FXOS Software 操作系统命令注入漏洞

(CNNVD-202010-1152)

Cisco FXOS Software 是美国思科（Cisco）公司的一套运行在思科安全设备中的防火墙软件。

Cisco FXOS 存在安全漏洞，该漏洞源于用户提供的命令的输入验证不足造成的。攻击者可利用该漏洞可以通过对设备进行身份验证并向受影响的命令提交精心设计的输入来利用此漏洞，在底层操作系统上使用 root 特权执行命令。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fxos-cmdinj-b63rwKPM>

5. Red Hat SPICE remote display system 缓冲区错误漏洞

(CNNVD-202010-194)

Red Hat SPICE remote display system 是美国红帽（Red Hat）公司的一个远程桌面控制系统。

Red Hat SPICE remote display system 中存在缓冲区错误漏洞。该漏洞源于网络系统或产品在内存上执行操作时，未正确验证数据边界，导致向关联的其他内存位置上执行了错误的读写操作。攻击者可利用该漏洞导致缓冲区溢出或堆溢出等。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://bugzilla.redhat.com/show_bug.cgi?id=1868435

6. Microsoft SharePoint 访问控制错误漏洞 (CNNVD-202010-478)

Microsoft SharePoint 是美国微软（Microsoft）公司的一套企业业务协作平台。该平台用于对业务信息进行整合，并能够共享工作、与他人协同工作、组织项目和工作组、搜索人员和信息。

Microsoft SharePoint 存在安全漏洞，该漏洞允许攻击者可以在 SharePoint 应用程序池和 SharePoint 服务器场帐户的上下文中运行任意代码。以下产品及版本受到影响： Microsoft SharePoint Enterprise Server 2016 版本， Microsoft SharePoint Foundation 2013 SP1 版本， Microsoft SharePoint Server 2019 版本。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

<https://support.microsoft.com/en-us/help/4486676/security-update-for-sharepoint-server-2019-october-13-2020>

7. Google Chrome 资源管理错误漏洞（CNNVD-202010-1458）

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。Blink 是美国谷歌（Google）公司和挪威欧朋（OperaSoftware）公司共同开发的一套浏览器排版引擎（渲染引擎）。PDFium 是其中的一个开源 PDF 渲染引擎。

chromium-browser 存在资源管理错误漏洞，该漏洞源于网络系统或产品对系统资源（如内存、磁盘空间、文件等）的管理不当。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://chromereleases.googleblog.com/2020/10/stable-channel-update-for-desktop_20.html

8. Linux kernel 输入验证错误漏洞（CNNVD-202010-133）

Linux kernel 是美国 Linux 基金会发布的开源操作系统 Linux 所使用的内核。KVM 是其中的一个基于内核的虚拟机。

Linux kernel 5.9-rc7 版本存在安全漏洞，该漏洞源于 HDLC PPP 模块发现了一个缺陷。内存损坏和读溢出是由 ppp cp 解析 cr 函数中不正确的输入验证引起的，攻击者可利用该漏洞导致系统崩溃或拒绝服务。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

<https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00021.html>

二、接报漏洞情况

本月接报漏洞 26286 个，其中信息技术产品漏洞（通用型漏洞）25 个，网络信息系统漏洞（事件型漏洞）26261 个。

表 7 2020 年 10 月漏洞接报情况

序号	报送单位	漏洞总量
1	网神信息技术（北京）股份有限公司	18149
2	上海斗象信息科技有限公司	4314
3	长春嘉诚信息技术股份有限公司	1103
4	中新网络信息安全股份有限公司	849
5	北京奇虎科技有限公司	355
6	北京微步在线科技有限公司	291
7	北京华云安信息技术有限公司	181
8	内蒙古奥创科技有限公司	128

9	山东华鲁科技发展股份有限公司	123
10	西安交大捷普网络科技有限公司	107
11	山东新潮信息技术有限公司	69
12	星云博创科技有限公司	64
13	西安四叶草信息技术有限公司	60
14	北京数字观星科技有限公司	59
15	北京天地和兴科技有限公司	50
16	广州锦行网络科技有限公司	40
17	北京启明星辰信息安全技术有限公司	31
18	深信服科技有限公司	31
19	中国电信股份有限公司网络安全产品运营中心	28
20	新华三技术有限公司	28
21	绿盟科技集团股份有限公司	20
22	远江盛邦（北京）网络安全科技股份有限公司	20
23	国防科技大学	18
24	上海安几科技有限公司	17
25	亚信科技（成都）有限公司	15
26	杭州默安科技有限公司	13
27	浙江国利网安科技有限公司	13
28	浪潮电子信息产业股份有限公司	12
29	湖南匡安网络技术有限公司	10
30	北京天融信网络安全技术有限公司	9
31	个人	9

32	北京赋云安运营科技有限公司	8
33	太极计算机股份有限公司	8
34	安徽华云网安信息技术有限公司	8
35	北京威努特技术有限公司	7
36	内蒙古洞明科技有限公司	6
37	广东东福信息技术有限公司	6
38	上海安识网络科技有限公司	5
39	北京智游网安科技有限公司	5
40	北京优炫软件股份有限公司	4
41	安徽长泰信息安全服务有限公司	3
42	中兴通讯	2
43	四川哨兵信息科技有限公司	2
44	深圳市魔方安全科技有限公司	2
45	长亭科技	2
46	上海大学机电工程与自动化学院	1
47	中国科学院软件研究所	1
48	信息工程大学	1
49	北京圣博润高新技术股份有限公司	1
50	北京山石网科信息技术有限公司	1
51	北京梆梆安全科技有限公司	1
52	北京蓝森科技有限公司	1
53	学生-安全爱好者	1
54	招商银行	1

55	重庆梦之想科技有限责任公司	1
报送总计		26286

三、重大漏洞预警

3.1 Oracle WebLogic 多个安全漏洞的预警

2020 年 10 月 21 日, Oracle 官方发布了多个安全漏洞的公告, 包括 Oracle WebLogic Server 安全漏洞 (CNNVD-202010-1008、CVE-2020-14882)、Oracle WebLogic Server Core 安全漏洞 (CNNVD-202010-1010、CVE-2020-14841)、Oracle WebLogic Server Core 安全漏洞 (CNNVD-202010-1006、CVE-2020-14825) 等多个漏洞。攻击者可利用漏洞在未授权的情况下发送攻击数据, 实现远程代码执行, 最终控制目标服务器。目前, Oracle 官方已经发布补丁修复了漏洞, 建议用户及时确认是否受到漏洞影响, 尽快采取修补措施。

.漏洞介绍

Oracle WebLogic Server 是美国甲骨文 (Oracle) 公司开发的一款适用于云环境和传统环境的应用服务中间件, 它提供了一个现代轻型开发平台, 支持应用从开发到生产的整个生命周期管理, 并简化了应用的部署和管理。T3 协议是用于在 WebLogic 服务器和其他类型的 Java 程序之间传输信息的协议。IIOP 协议是一个用于 CORBA 2.0 及兼容平台, 用来在 CORBA 对象请求代理之间交流的协议。

2020 年 10 月 21 日，Oracle 官方发布了大量安全补丁，共 421 个，涉及 Weblogic 多个远程代码执行漏洞。其中部分漏洞和 T3、IIOP 协议有关，可造成远程代码执行，具体请参考 <https://www.oracle.com/security-alerts/cpujan2020.html>，部分重要漏洞如下：

	漏洞名称	漏洞编号	影响版本
1	Oracle WebLogic Server 安全漏洞	CNNVD-202010-1008 CVE-2020-14882	Weblogic Server 10.3.6.0.0 Weblogic Server 12.1.3.0.0 Weblogic Server 12.2.1.3.0 Weblogic Server 12.2.1.4.0 Weblogic Server 14.1.1.0.0
2	Oracle WebLogic Server Core 安全漏洞	CNNVD-202010-1010 CVE-2020-14841	Weblogic Server 10.3.6.0.0 Weblogic Server 12.1.3.0.0 Weblogic Server 12.2.1.3.0 Weblogic Server 12.2.1.4.0 Weblogic Server 14.1.1.0.0
3	Oracle WebLogic Server Core 安全漏洞	CNNVD-202010-1006	Weblogic Server 12.2.1.3.0

		CVE-2020-14825	Weblogic Server 12.2.1.4.0 Weblogic Server 14.1.1.0.0
4	Oracle WebLogic Server Core 安全漏洞	CNNVD-202010-1005 CVE-2020-14859	Weblogic Server 10.3.6.0.0 Weblogic Server 12.1.3.0.0 Weblogic Server 12.2.1.3.0 Weblogic Server 12.2.1.4.0 Weblogic Server 14.1.1.0.0
5	Oracle WebLogic Server 安全漏洞	CNNVD-202010-994 CVE-2020-14820	Weblogic Server 10.3.6.0.0 Weblogic Server 12.1.3.0.0 Weblogic Server 12.2.1.3.0 Weblogic Server 12.2.1.4.0 Weblogic Server 14.1.1.0.0

.危害影响

攻击者可利用漏洞在未授权的情况下发送攻击数据,实现远程代码执行,最终控制 WebLogic 服务器。

.修复建议

目前, Oracle 官方已经发布补丁修复了漏洞,建议用户及时确认是否受到漏洞影响,尽快采取修补措施。Oracle 官方更新链接如下:

<https://www.oracle.com/security-alerts/cpujul2020.html>

3.2 Vmware ESXi 安全漏洞的预警

近日,国家信息安全漏洞库(CNNVD)收到关于 Vmware ESXi 安全漏洞(CNNVD-202010-966、CVE-2020-3992)情况的报送。成功利用漏洞的攻击者可以在无需管理员授权的情况下在目标服务器上执行系统命令,获取服务器系统权限,最终控制目标服务器。Vmware ESXi 6.5、ESXi 6.7、ESXi 7.0、VMware Cloud Foundation (ESXi) 3.x、VMware Cloud Foundation (ESXi) 4.x 均受此漏洞影响。目前官方已在最新版本中修复了该漏洞,建议用户及时确认是否受到漏洞影响,尽快采取修补措施。

.漏洞介绍

VMware ESXi 是美国 VMware 公司的一套可直接安装在物理服务器上的服务器虚拟化平台。Vmware ESXi 存在一个可以远程代码执行的安全漏洞,攻击者可通过访问 ESXi 宿主机上的 427 端口触发

OpenSLP 服务中的“use-after-free”，从而导致远程代码执行，获取服务器系统权限，最终控制目标服务器。

.危害影响

成功利用漏洞的攻击者可以在无需管理员授权的情况下在目标服务器上执行系统命令，获取服务器系统权限，最终控制目标服务器。

Vmware ESXi 6.5、ESXi 6.7、ESXi 7.0、VMware Cloud Foundation (ESXi) 3.x、VMware Cloud Foundation (ESXi) 4.x 均受此漏洞影响。

.修复建议

目前官方已在最新版本中修复了该漏洞，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。官方链接如下：

[https://www.vmware.com/security/advisories/VMSA-2020-0023.ht
ml](https://www.vmware.com/security/advisories/VMSA-2020-0023.html)