北京师范大学网络信息安全通告

2020 年 7 月报告

北京师范大学信息网络中心

2020 年 8 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 4
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 5
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 15
2. 接报漏洞情况 25
3. 重大漏洞预警 27
3.1. 微软多个安全漏洞的预警 27
3.2. Oracle WebLogic 多个安全漏洞的预警 32

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 7 月份新增安全漏洞共 1470 个，从厂商分布来看，Oracle 公司产品的漏洞数量最多，共发布 213 个；从漏洞类型来看，跨站脚本类的漏洞占比最大，达到 10.88%。本月新增漏洞中，超危漏洞 215 个、高危漏洞 569 个、中危漏洞 637 个、低危漏洞 46 个，相应修复率分别为 66.05%、86.99%、87.28%以及 84.78%。合计 1232 个漏洞已有修复补丁发布，本月整体修复率 83.98%。

截至 2020 年 7 月 31 日，CNNVD 采集漏洞总量已达 148611 个。

1.1 漏洞增长概况

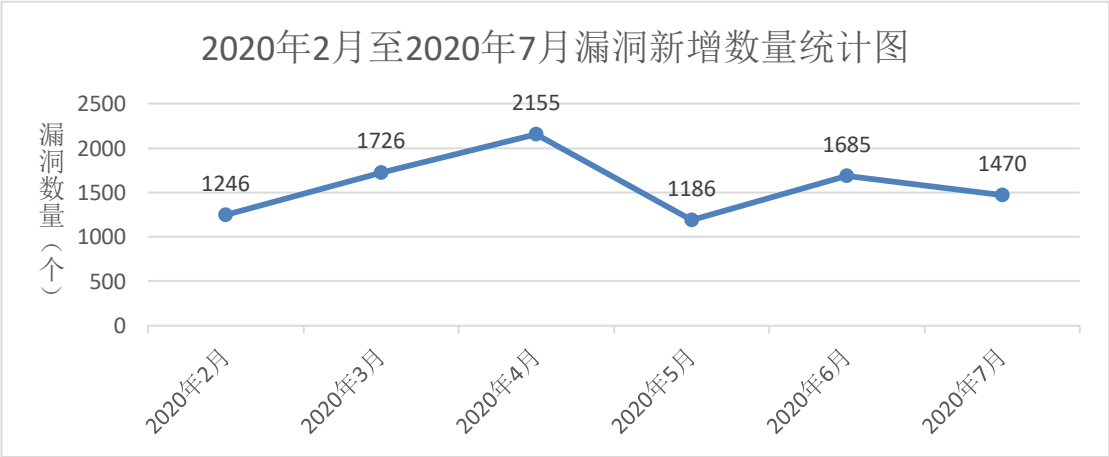

图 1 2020 年 2 月至 2020 年 7 月漏洞新增数量统计图

2020 年 7 月新增安全漏洞 1470 个，与上月（1685 个）相比减少了 12.76%。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 1578 个。

1.2 漏洞分布情况

1.2.1 漏洞厂商分布

7 月厂商漏洞数量分布情况如表 1 所示，Oracle 公司漏洞达到 213 个，占本月漏洞总量的 14.49%。

表 1　2020 年 7 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	213	14.49%
2	Microsoft	123	8.37%
3	IBM	56	3.81%
4	Cisco	54	3.67%
5	Google	46	3.13%
6	Apple	45	3.06%
7	Adobe	35	2.38%
8	CloudBees	28	1.90%
9	Huawei	27	1.84%
10	Mozilla 基金会	26	1.77%

1.2.2 漏洞产品分布

7 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 93 个，其中 Windows 10 漏洞数量最多，共 84 个，占主流操作系统漏洞总量的 15.58%，排名第一。

表 2　2020 年 7 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	84
2	Windows Server 2019	81
3	Windows Server 2016	69

4	Windows Server 2012	47
5	Windows Server 2012 R2	47
6	Windows Server 2008	41
7	Windows Server 2008 R2	41
8	Windows 8.1	39
9	Windows Rt 8.1	39
10	Windows 7	34
11	Android	10
12	Linux Kernel	7

*由于 Windows 整体市占率高达百分之九十以上，所以上表针对不同的 Windows 版本分别进行统计

*上表漏洞数量为影响该版本的漏洞数量，由于同一漏洞可能影响多个版本操作系统，计算某一系列操作系统漏洞总量时，不能对该系列所有操作系统漏洞数量进行简单相加。

1.2.3 漏洞类型分布

7 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 10.88%。

表 3 2020 年 7 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	160	10.88%
2	缓冲区错误	135	9.18%
3	信息泄露	78	5.31%
4	输入验证错误	77	5.24%
5	代码问题	70	4.76%
6	操作系统命令注入	58	3.95%
7	资源管理错误	49	3.33%
8	SQL 注入	49	3.33%
9	授权问题	41	2.79%
10	路径遍历	33	2.24%
11	注入	30	2.04%
12	访问控制错误	25	1.70%
13	信任管理问题	22	1.50%
14	跨站请求伪造	18	1.22%
15	加密问题	8	0.54%
16	数据伪造问题	7	0.48%

17	代码注入	7	0.48%
18	后置链接	6	0.41%
19	竞争条件问题	6	0.41%
20	权限许可和访问控制问题	4	0.27%
21	日志信息泄露	4	0.27%
22	数字错误	4	0.27%
23	命令注入	3	0.20%
24	环境问题	1	0.07%
25	参数注入	1	0.07%
26	其他	574	39.05%

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。7 月漏洞危害等级分布如图 2 所示，其中超危漏洞 215 条，占本月漏洞总数的 14.66%。

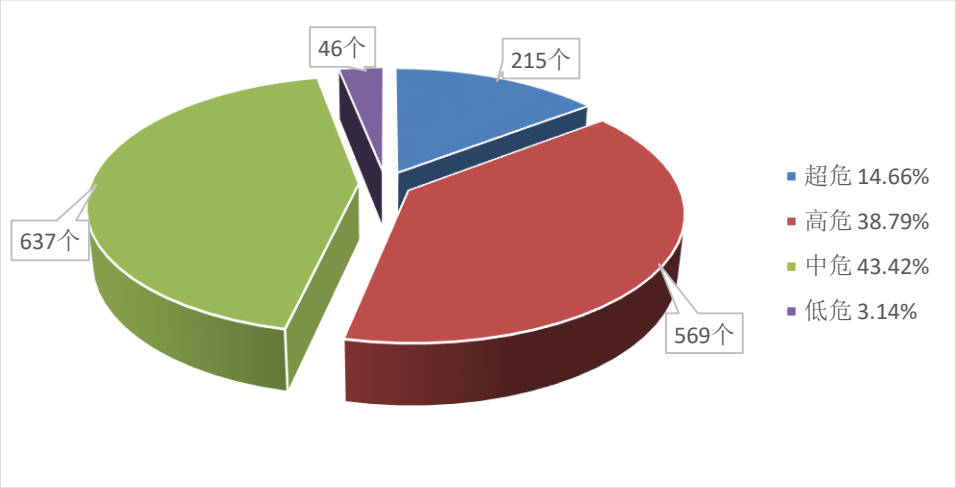

图 2　2020 年 7 月漏洞危害等级分布

1.3 漏洞修复情况

1.3.1 整体修复情况

7 月漏洞修复情况按危害等级进行统计见图 3。其中中危漏洞修复率最高，达到 87.28%，超危漏洞修复率最低，比例为 66.05%。总体来看，本月整体修复率，由上月的 85.70%下降至本月的 83.98%。

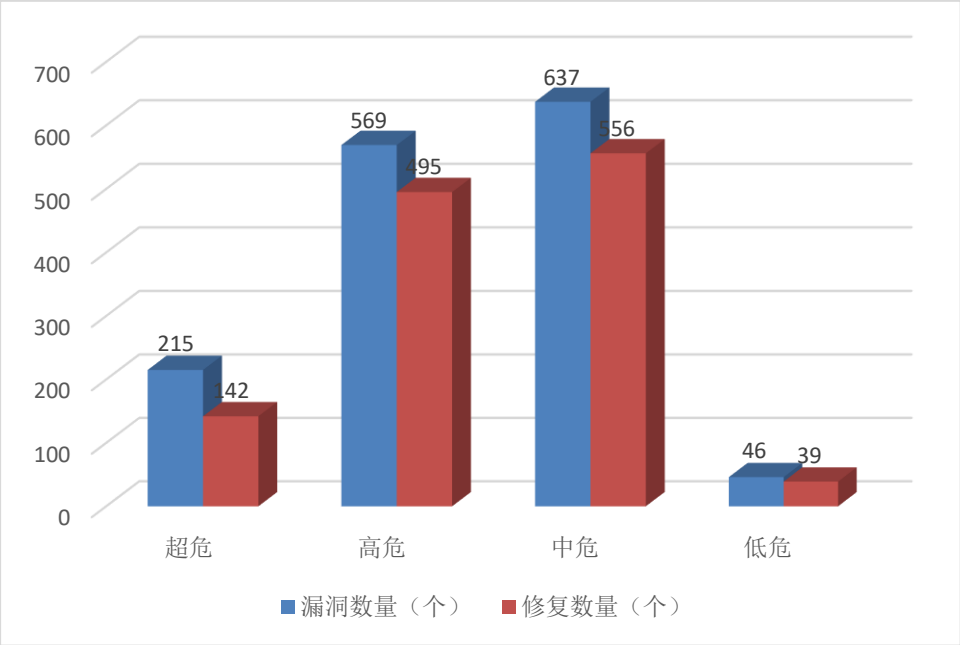

图 3 2020 年 7 月漏洞修复数量统计

1.3.2 厂商修复情况

7 月漏洞修复情况按漏洞数量前十厂商进行统计，其中 Oracle、Microsoft、IBM 等十个厂商共 653 条漏洞，占本月漏洞总数的 44.42%，漏洞修复率为 97.55%，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、Microsoft、Google、Apple、Adobe、Huawei、Mozilla 基金会等公司本月漏洞修复率均为 100%，共 637 条漏洞已全部修复。

表 4　2020 年 7 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	213	213	100.00%
2	Microsoft	123	123	100.00%
3	IBM	56	55	98.21%
4	Cisco	54	51	94.44%
5	Google	46	46	100.00%
6	Apple	45	45	100.00%
7	Adobe	35	35	100.00%
8	CloudBees	28	16	57.14%
9	Huawei	27	27	100.00%
10	Mozilla 基金会	26	26	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 215 个，其中重要漏洞实例如表 5 所示。

表 5　2020 年 7 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-202007-968	Advantech	Apache Kylin SQL 注入漏洞（CNNVD-202007-770）
		CNNVD-202007-770	Apache 软件基金会	
		CNNVD-202007-519	Sophos	
		CNNVD-202007-349	SpryMedia	
		CNNVD-202007-352		
		CNNVD-202007-353		
		CNNVD-202007-343	WebChess 项目	
		CNNVD-202007-153	个人开发者	
2	缓冲区错误	CNNVD-202007-944	AMD	Microsoft Windows Server DNS Server 缓冲区错误漏洞（CNNVD-202007-864）
		CNNVD-202007-953		
		CNNVD-202007-972		
		CNNVD-202007-1596	Artifex Software	
		CNNVD-202007-1136	Cisco	
		CNNVD-202007-1149		
		CNNVD-202007-1725		
		CNNVD-202007-1374	D-Link	
		CNNVD-202007-407	FreeBSD 基金会	
		CNNVD-202007-374	GeoVision	

		CNNVD-202007-272	Google	
		CNNVD-202007-273		
		CNNVD-202007-278		
		CNNVD-202007-1648	HMS Networks	
		CNNVD-202007-1361	Lua 团队	
		CNNVD-202007-864	Microsoft	
		CNNVD-202007-304	Mitsubishi Electric	
		CNNVD-202007-948	Moxa	
		CNNVD-202007-1360	mruby	
		CNNVD-202007-061	Ntop	
		CNNVD-202007-068		
		CNNVD-202007-070		
		CNNVD-202007-071		
		CNNVD-202007-275	Qualcomm	
		CNNVD-202007-340	RIOT	
		CNNVD-202007-1591	Ruckus Networks	
		CNNVD-202007-821	Siemens	
		CNNVD-202007-848		
		CNNVD-202007-1654	Softing Industrial Automation	
		CNNVD-202007-1560	The Trusted Domain 项目	
3	跨站脚本	CNNVD-202007-361	Qualcomm	Adobe Magento Commerce 和 Magento Open Source 跨站脚本漏洞（CNNVD-202007-1646）
		CNNVD-202007-1646	Adobe	
		CNNVD-202007-560	Artica	
		CNNVD-202007-1099	LibreHealth	
		CNNVD-202007-1673	Gambio	
		CNNVD-202007-1672	Adobe	
		CNNVD-202007-965	Advantech	
		CNNVD-202007-1589	Dell	
		CNNVD-202007-1408	INNEO Solutions	
		CNNVD-202007-1364	Pritunl	
		CNNVD-202007-1528	Riverbed Technology	
		CNNVD-202007-1271	rollup-plugin-serve 项目	
4	其他	CNNVD-202007-989	Adobe	Oracle Fusion Middleware WebLogic Server 安全漏洞（CNNVD-202007-825）
		CNNVD-202007-992		
		CNNVD-202007-1080	Apple	
		CNNVD-202007-1409	AvertX	
		CNNVD-202007-1268	Bflysoft	

		CNNVD-202007-1629	CentOS Web Panel	
		CNNVD-202007-1413	Claws Mail 项目	
		CNNVD-202007-427	Eclipse 基金会	
		CNNVD-202007-1153		
		CNNVD-202007-281	Google	
		CNNVD-202007-408		
		CNNVD-202007-982		
		CNNVD-202007-1658	Grin	
		CNNVD-202007-1671	IBM	
		CNNVD-202007-412	Juniper Networks	
		CNNVD-202007-1722	KubeVirt 项目	
		CNNVD-202007-346	libp2p 项目	
		CNNVD-202007-091	Linkplay	
		CNNVD-202007-094		
		CNNVD-202007-378	Micro Focus	
		CNNVD-202007-592	Microsoft	
		CNNVD-202007-1511	Mida Solutions	
		CNNVD-202007-291	MobileIron	
		CNNVD-202007-086	Monsta	
		CNNVD-202007-1386	Nagios	
		CNNVD-202007-1676	NCP engineering	
		CNNVD-202007-1707	NEC	
		CNNVD-202007-1708		
		CNNVD-202007-1713		
		CNNVD-202007-1369	Open Microscopy Environment 团队	
		CNNVD-202007-1584	OpenBSD 项目组	
		CNNVD-202007-284	OpenJS 基金会	
		CNNVD-202007-287		
		CNNVD-202007-818	Oracle	
		CNNVD-202007-820		
		CNNVD-202007-823		
		CNNVD-202007-825		
		CNNVD-202007-922		
		CNNVD-202007-923		
		CNNVD-202007-924		
		CNNVD-202007-925		
		CNNVD-202007-947		
		CNNVD-202007-949		
		CNNVD-202007-960		
		CNNVD-202007-1520	Parallels	
		CNNVD-202007-1264	Python 软件基金会	

		CNNVD-202007-1585	rConfig	
		CNNVD-202007-1674	Secomea	
		CNNVD-202007-1641	TYPO3 协会	
		CNNVD-202007-1095	uFactory	
		CNNVD-202007-1128		
		CNNVD-202007-310	Venki	
		CNNVD-202007-099	WAVLINK	
5	授权问题	CNNVD-202007-103	Cisco	多款 Cisco 产品授权问题漏洞（CNNVD-202007-103）
		CNNVD-202007-1143		
		CNNVD-202007-1704		
		CNNVD-202007-1175	ConnectWise	
		CNNVD-202007-1406	DevSpace	
		CNNVD-202007-1029	Fortinet	
		CNNVD-202007-289	MobileIron	
		CNNVD-202007-170	PrestaShop	
		CNNVD-202007-800	SAP	
		CNNVD-202007-1316	ZTE	
		CNNVD-202007-178	个人开发者	
		CNNVD-202007-182		
6	输入验证错误	CNNVD-202007-958	Advantech	Microsoft Windows Hyper-V RemoteFX vGPU 安全漏洞（CNNVD-202007-893）
		CNNVD-202007-956	AMD	
		CNNVD-202007-1090	Cisco	
		CNNVD-202007-572	KDE、Apple、Google 等	
		CNNVD-202007-887	Microsoft	
		CNNVD-202007-888		
		CNNVD-202007-891		
		CNNVD-202007-893		
		CNNVD-202007-895		
		CNNVD-202007-897		
		CNNVD-202007-276	Qualcomm	
		CNNVD-202007-132	Tobesoft	
		CNNVD-202007-133		
7	信任管理问题	CNNVD-202007-1166	ABB	Cisco Prime License Manager Software 信任管理问题漏洞（CNNVD-202007-1129）
		CNNVD-202007-1129	Cisco	
		CNNVD-202007-1156		
		CNNVD-202007-1703		
		CNNVD-202007-1350	IBM	
		CNNVD-202007-832	OpenLDAP 基金会	
		CNNVD-202007-1657	Secomea	
		CNNVD-202007-1662		
		CNNVD-202007-565	Tenda	

8	注入	CNNVD-202007-961	Advantech	Atlassian JIRA Server 和 Data Center 注入漏洞（CNNVD-202007-220）
		CNNVD-202007-220	Atlassian	
		CNNVD-202007-309	Mitsubishi Electric	
		CNNVD-202007-871	Netflix	
		CNNVD-202007-514	Raonwiz	
		CNNVD-202007-1407	RaspberryTortoise	
		CNNVD-202007-863	SuperWebMailer	
		CNNVD-202007-564	Tenda	
		CNNVD-202007-516	Tobesoft	
		CNNVD-202007-097	WAVLINK	
		CNNVD-202007-080	个人开发者	
		CNNVD-202007-518		
		CNNVD-202007-1272		

1. Apache Kylin SQL 注入漏洞（CNNVD-202007-770）

Apache Kylin 是美国阿帕奇（Apache）软件基金会的一款开源的分布式分析型数据仓库。该产品主要提供 Hadoop/Spark 之上的 SQL 查询接口及多维分析（OLAP）等功能。

Apache Kylin 中存在 SQL 注入漏洞。该漏洞源于基于数据库的应用缺少对外部输入 SQL 语句的验证。攻击者可利用该漏洞执行非法 SQL 命令。以下产品及版本受到影响：Apache Kylin 2.0.0 版本，2.1.0 版本，2.2.0 版本，2.3.0 版本，2.3.1 版本，2.3.2 版本，2.4.0 版本，2.4.1 版本，2.5.0 版本，2.5.1 版本，2.5.2 版本，2.6.0 ，2.6.1 版本，2.6.2 版本，2.6.3 版本，2.6.4 版本，2.6.5 版本，2.6.6 版本，3.0.0-alpha 版本，3.0.0-alpha2 版本，3.0.0-beta 版本，3.0.0 版本，3.0.1 版本，3.0.2 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://lists.apache.org/thread.html/r63d5663169e866d44ff92507961

93337cff7d9cf61cc3839e86163fd%40%3Cuser.kylin.apache.org%3E

2. Microsoft Windows Server DNS Server 缓冲区错误漏洞（CNNVD-202007-864）

Microsoft Windows Server 是美国微软（Microsoft）公司的一套服务器操作系统。Windows DNS Server 是其中的一个 DNS（域名系统）服务器。

Microsoft Windows DNS Server 中存在缓冲区错误漏洞，该漏洞源于程序无法正确处理请求。攻击者可通过发送恶意的请求利用该漏洞在本地系统帐户的上下文中运行任意代码。以下产品及版本受到影响：Windows Server 2008 SP2，Windows Server 2008 R2 SP1，Windows Server 2012，Windows Server 2012 R2，Windows Server 2016，Windows Server 2019，Windows Server 1903 版本，Windows Server 1909 版本，Windows Server 2004 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://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1350

3. Adobe Magento Commerce 和 Magento Open Source 跨站脚本漏洞（CNNVD-202007-1646）

Adobe Magento 是美国奥多比（Adobe）公司的一套开源的 PHP 电子商务系统。该系统提供权限管理、搜索引擎和支付网关等功能。Magento Open Source 是 Magento 的开源版本。Magento Commerce 是 Magento 的商业版本。

Adobe Magento Commerce 2 2.3.5-p1及之前版本和Magento Open Source 2 2.3.5-p1 及之前版本中存在跨站脚本漏洞。攻击者可利用该漏洞执行任意代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://helpx.adobe.com/security/products/magento/apsb20-47.html

4. **Oracle Fusion Middleware WebLogic Server 安全漏洞（CNNVD-202007-825）**

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。该平台提供了中间件、软件集合等功能。WebLogic Server 是其中的一个适用于云环境和传统环境的应用服务器组件。

Oracle Fusion Middleware 中的 WebLogic Server 12.2.1.3.0 版本，12.2.1.4.0 版本和 14.1.1.0.0 版本的 Core 组件存在安全漏洞。攻击者可利用该漏洞控制 Oracle WebLogic Server，影响数据的可用性、保密性和完整性。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

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

5. **多款 Cisco 产品授权问题漏洞（CNNVD-202007-103）**

Cisco Small Business 200 Series Smart Switches 等都是美国思科（Cisco）公司的产品。Cisco Small Business 200 Series Smart Switches 是一款小型智能交换机设备。Cisco 350 Series Managed Switches 是一款 350 系列管理型交换机。550X Series Stackable Managed Switches

是一款 550X 系列管理型交换机。

多款 Cisco 产品中 Web 接口的会话管理存在授权问题漏洞。攻击者可利用该漏洞绕过身份验证保护，获取被劫持会话账户的权限，包括管理员权限。以下产品及版本受到影响：Cisco 250 Series Smart Switches；350 Series Managed Switches；350X Series Stackable Managed Switches；550X Series Stackable Managed Switches；Small Business 200 Series Smart Switches；Small Business 300 Series Managed Switches；Small Business 500 Series Stackable Managed Switches。

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-sbswitch-session-JZAS5jnY

6. Microsoft Windows Hyper-V RemoteFX vGPU 安全漏洞（CNNVD-202007-893）

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。Windows Hyper-V 是其中的一个虚拟化产品，支持在 Windows 中创建虚拟机。

Microsoft Hyper-V RemoteFX vGPU 中存在远程代码执行漏洞，该漏洞源于程序无法正确验证虚拟机操作系统上的已通过身份验证的用户的输入。攻击者可通过在虚拟机操作系统上运行特制的应用程序利用该漏洞在主机操作系统执行任意代码。以下产品及版本受到影

响：Windows Server 2008 R2 SP1，Windows Server 2012，Windows Server 2012 R2，Windows Server 2016。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1041

7. Cisco Prime License Manager Software 信任管理问题漏洞（CNNVD-202007-1129）

Cisco Prime License Manager Software 是美国思科（Cisco）公司的一套用于 Cisco 产品的许可证管理软件。

Cisco Prime License Manager（PLM）Software10.5(2)SU9 及之前版本和 11.5(1)SU6 及之前版本中的 Web 管理界面存在信任管理问题漏洞，该漏洞源于程序没有正确验证用户输入。远程攻击者可借助恶意请求利用该漏洞获取系统管理权限。

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-cisco-prime-priv-esc-HyhwdzBA

8. Atlassian JIRA Server 和 Data Center 注入漏洞（CNNVD-202007-220）

Atlassian JIRA Server 和 Atlassian JIRA Data Center 都是澳大利亚 Atlassian 公司的产品。Atlassian JIRA Server 是一套缺陷跟踪管理系统的服务器版本。该系统主要用于对工作中各类问题、缺陷进行跟踪管理。Atlassian JIRA Data Center 是 Atlassian JIRA 的数据中心版本。

Atlassian JIRA Server 和 Data Center 中的 velocity 模板的使用方法存在注入漏洞，该漏洞源于不安全的反序列化。远程攻击者可利用该漏洞执行代码。以下产品及版本受到影响：Atlassian JIRA Server 7.13.0 之前版本，8.5.0 之前的 8.0.0 版本，8.8.1 之前的 8.6.0 版本；Atlassian JIRA Data Center 7.13.0 之前版本，8.5.0 之前的 8.0.0 版本，8.8.1 之前的 8.6.0 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://www.atlassian.com/

1.4.2 高危漏洞实例

本月高危漏洞共 569 个，其中重点漏洞实例如表 6 所示。

表 6　2020 年 7 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-202007-1310	ArticaTech	VMware VeloCloud Orchestrator SQL 注入漏洞（CNNVD-202007-373）
		CNNVD-202007-1623	CentOS Web Panel	
		CNNVD-202007-1624		
		CNNVD-202007-1625		
		CNNVD-202007-1626		
		CNNVD-202007-1627		
		CNNVD-202007-1628		
		CNNVD-202007-1630		
		CNNVD-202007-1631		
		CNNVD-202007-1632		
		CNNVD-202007-1634		
		CNNVD-202007-1635		
		CNNVD-202007-1636		
		CNNVD-202007-350	ConnectWise	
		CNNVD-202007-520	Glacies 团队	
		CNNVD-202007-421	Klemen Stirn	
		CNNVD-202007-1512	Mida Solutions	
		CNNVD-202007-1394	Munkireport 项目	

		CNNVD-202007-1395		
		CNNVD-202007-1396		
		CNNVD-202007-395	phpList	
		CNNVD-202007-1587	rConfig	
		CNNVD-202007-1640		
		CNNVD-202007-837	Siemens	
		CNNVD-202007-561	SRS Simple Hits Counter 项目	
		CNNVD-202007-1283	Teclib	
		CNNVD-202007-373	VMware	
2	代码问题	CNNVD-202007-1015	Adobe	Microsoft 365 Apps for Enterprise 代码问题漏洞（CNNVD-202007-577）
		CNNVD-202007-1017		
		CNNVD-202007-1304	ASUS	
		CNNVD-202007-219	Atlassian	
		CNNVD-202007-1351	Bitwarden	
		CNNVD-202007-1563	Cherokee 项目	
		CNNVD-202007-1061	Cisco	
		CNNVD-202007-1079		
		CNNVD-202007-1192	ClamAV 团队	
		CNNVD-202007-158	CloudBees	
		CNNVD-202007-1032	Eclipse 基金会	
		CNNVD-202007-559	Embedthis Software	
		CNNVD-202007-523	Facebook	
		CNNVD-202007-1176	GNU	
		CNNVD-202007-093	Huawei	
		CNNVD-202007-394	IBM	
		CNNVD-202007-1168		
		CNNVD-202007-1173		
		CNNVD-202007-1118	IceWarp	
		CNNVD-202007-1521	Lenovo	
		CNNVD-202007-1522		
		CNNVD-202007-1300	Liferay	
		CNNVD-202007-577	Microsoft	
		CNNVD-202007-840		
		CNNVD-202007-941		
		CNNVD-202007-306	Mitsubishi Electric	
		CNNVD-202007-116	Mozilla 基金会	
		CNNVD-202007-860	OpenVPN	
		CNNVD-202007-1680	PortlandLabs	
		CNNVD-202007-360	Qualcomm	

		CNNVD-202007-804	SAP	
		CNNVD-202007-808		
		CNNVD-202007-1111	SecZetta	
		CNNVD-202007-1147	SilverStripe	
		CNNVD-202007-1306	Transloadit	
		CNNVD-202007-1123	Trend Micro	
		CNNVD-202007-375	Veeam	
		CNNVD-202007-376		
		CNNVD-202007-172	个人开发者	
		CNNVD-202007-1356	奇虎科技	
		CNNVD-202007-1357		
		CNNVD-202007-1359		
3	缓冲区错误	CNNVD-202007-249	Adobe	Adobe Bridge 缓冲区错误漏洞（CNNVD-202007-1326）
		CNNVD-202007-995		
		CNNVD-202007-997		
		CNNVD-202007-1326		
		CNNVD-202007-1327		
		CNNVD-202007-1328		
		CNNVD-202007-1329		
		CNNVD-202007-1330		
		CNNVD-202007-1332		
		CNNVD-202007-1333		
		CNNVD-202007-1334		
		CNNVD-202007-1335		
		CNNVD-202007-1337		
		CNNVD-202007-570	Apache 软件基金会	
		CNNVD-202007-1088	Apple	
		CNNVD-202007-1307	Automattic	
		CNNVD-202007-524	Bareos	
		CNNVD-202007-1081	Cisco	
		CNNVD-202007-1083		
		CNNVD-202007-001	Envoy 项目	
		CNNVD-202007-1185	Foxit	
		CNNVD-202007-1177	GNU	
		CNNVD-202007-1179		
		CNNVD-202007-1181		
		CNNVD-202007-1182		
		CNNVD-202007-964	Google	
		CNNVD-202007-969		
		CNNVD-202007-977		
		CNNVD-202007-978		
		CNNVD-202007-980		

		CNNVD-202007-987		
		CNNVD-202007-996		
		CNNVD-202007-1008		
		CNNVD-202007-1016		
		CNNVD-202007-1553		
		CNNVD-202007-1087	Huawei	
		CNNVD-202007-1297	Human Talk	
		CNNVD-202007-425	Juniper Networks	
		CNNVD-202007-078	LEAD Technologies	
		CNNVD-202007-583	Microsoft	
		CNNVD-202007-587		
		CNNVD-202007-594		
		CNNVD-202007-601		
		CNNVD-202007-619		
		CNNVD-202007-622		
		CNNVD-202007-623		
		CNNVD-202007-628		
		CNNVD-202007-629		
		CNNVD-202007-649		
		CNNVD-202007-712		
		CNNVD-202007-785		
		CNNVD-202007-793		
		CNNVD-202007-690		
		CNNVD-202007-111	Mozilla 基金会	
		CNNVD-202007-113		
		CNNVD-202007-119		
		CNNVD-202007-1642	NETGEAR	
		CNNVD-202007-1647		
		CNNVD-202007-1651		
		CNNVD-202007-063	Ntop	
		CNNVD-202007-672	Oracle	
		CNNVD-202007-072	Phoenix Contact	
		CNNVD-202007-073		
		CNNVD-202007-263	Qualcomm	
		CNNVD-202007-269		
		CNNVD-202007-271		
		CNNVD-202007-279	Realtek	
		CNNVD-202007-811	Siemens	
		CNNVD-202007-1124	Trend Micro	
		CNNVD-202007-222	Veeam	
4	跨站脚本	CNNVD-202007-1323	Moodle	Oracle Fusion

		CNNVD-202007-807	Oracle	Middleware BI Publisher 跨站脚本漏洞（CNNVD-202007-807）
		CNNVD-202007-810		
		CNNVD-202007-902		
		CNNVD-202007-910		
		CNNVD-202007-912		
5	输入验证错误	CNNVD-202007-351	AutomationDirect	Microsoft Windows Font Library 输入验证错误漏洞（CNNVD-202007-600）
		CNNVD-202007-1086	Cisco	
		CNNVD-202007-1114		
		CNNVD-202007-1378		
		CNNVD-202007-1696		
		CNNVD-202007-363	Citrix Systems	
		CNNVD-202007-385	Huawei	
		CNNVD-202007-387		
		CNNVD-202007-388		
		CNNVD-202007-401	Juniper Networks	
		CNNVD-202007-409		
		CNNVD-202007-413		
		CNNVD-202007-415		
		CNNVD-202007-417		
		CNNVD-202007-418		
		CNNVD-202007-138	LibRaw 团队	
		CNNVD-202007-1106	LibreHealth	
		CNNVD-202007-096	Linkplay	
		CNNVD-202007-1043	lodash	
		CNNVD-202007-600	Microsoft	
		CNNVD-202007-615		
		CNNVD-202007-699		
		CNNVD-202007-1324	Moodle	
		CNNVD-202007-266	Qualcomm	
		CNNVD-202007-1592	Ruckus Networks	
		CNNVD-202007-1348	Sails	
		CNNVD-202007-121	Samba 团队	
		CNNVD-202007-1420	Schneider Electric	
		CNNVD-202007-1276	SonicWall	
6	信息泄露	CNNVD-202007-550	Atlassian	IBM Maximo Asset Management 信息泄露漏洞（CNNVD-202007-1688）
		CNNVD-202007-382	Broadcom	
		CNNVD-202007-404	D-Link	
		CNNVD-202007-1376		
		CNNVD-202007-130	DuckDuckGo	
		CNNVD-202007-270	Google	
		CNNVD-202007-1688	IBM	

		CNNVD-202007-064	Journal theme	
		CNNVD-202007-227	McAfee	
		CNNVD-202007-1183	Microweber 社区	
		CNNVD-202007-290	MobileIron	
		CNNVD-202007-792	Oracle	
		CNNVD-202007-1684	Red Hat	
		CNNVD-202007-1594	Ruckus Networks	
		CNNVD-202007-1410	Schneider Electric	
		CNNVD-202007-1142	SilverStripe	
		CNNVD-202007-316	SolarWinds	
		CNNVD-202007-1399	Wind River Systems	
7	注入	CNNVD-202007-1018	Adobe	Adobe Download Manager 注入漏洞（CNNVD-202007-1018）
		CNNVD-202007-381	Apache 软件基金会	
		CNNVD-202007-1543	Encode OSS	
		CNNVD-202007-1098	Huawei	
		CNNVD-202007-386	Mercari	
		CNNVD-202007-591	Microsoft	
		CNNVD-202007-782	Oracle	
		CNNVD-202007-1282	Western Digital	
		CNNVD-202007-297	个人开发者	
8	资源管理错误	CNNVD-202007-1102	Cisco	Google Chrome Developer Tools 资源管理错误漏洞（CNNVD-202007-993）
		CNNVD-202007-002	Envoy 项目	
		CNNVD-202007-003		
		CNNVD-202007-004		
		CNNVD-202007-399	FreeBSD 基金会	
		CNNVD-202007-993	Google	
		CNNVD-202007-1002		
		CNNVD-202007-1551		
		CNNVD-202007-1555		
		CNNVD-202007-1557		
		CNNVD-202007-081	Huawei	
		CNNVD-202007-089		
		CNNVD-202007-419	Juniper Networks	
		CNNVD-202007-1358	Lua 团队	
		CNNVD-202007-647	Microsoft	
		CNNVD-202007-308	Mitsubishi Electric	
		CNNVD-202007-109	Mozilla 基金会	
		CNNVD-202007-112		
		CNNVD-202007-115		

		CNNVD-202007-260	Qualcomm	
		CNNVD-202007-267		
		CNNVD-202007-125	Samba 团队	
		CNNVD-202007-573	Siemens	
		CNNVD-202007-582		
		CNNVD-202007-1652	Softing Industrial Automation	
		CNNVD-202007-301	英国剑桥大学	

1. VMware VeloCloud Orchestrator SQL 注入漏洞

（CNNVD-202007-373）

VMware VeloCloud Orchestrator 是美国威睿（VMware）公司的一套 NSX SD-WAN 解决方案的管理平台。该平台支持集中式配置、实时监控和故障排除等。

VMware VeloCloud Orchestrator 3.x 版本中存在安全漏洞，该漏洞源于程序没有正确验证输入。攻击者可借助特制 SQL 查询利用该漏洞获取特权数据。

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.velocloud.com/

2. Microsoft 365 Apps for Enterprise 代码问题漏洞

（CNNVD-202007-577）

Microsoft Office 是美国微软（Microsoft）公司的一款办公软件套件产品。该产品常用组件包括 Word、Excel、Access、Powerpoint、FrontPage 等。

Microsoft 365 Apps for Enterprise 中存在远程代码执行漏洞，该漏洞源于程序在加载动态链接库 (DLL) 文件前没有正确验证输入。

攻击者可通过诱使用户打开特制 Office 文档利用该漏洞控制受影响的系统。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1458

3. Adobe Bridge 缓冲区错误漏洞（CNNVD-202006-648）

Adobe Bridge 是美国奥多比（Adobe）公司的一款文件查看器。

基于 Windows 平台的 Adobe Bridge 10.0.3 及之前版本中存在安全漏洞。攻击者可利用该漏洞执行任意代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://helpx.adobe.com/security/products/bridge/apsb20-44.html

4. Oracle Fusion Middleware BI Publisher 跨站脚本漏洞（CNNVD-202007-807）

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。该平台提供了中间件、软件集合等功能。BI Publisher（前称 XML Publisher）是其中的一个报表组件。

Oracle Fusion Middleware 中的 BI Publisher 11.1.1.9.0 版本，12.2.1.3.0 版本和 12.2.1.4.0 版本的 Mobile Service 组件存在安全漏洞。攻击者可利用该漏洞未授权访问、更新、插入或删除数据，影响数据的保密性和完整性。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

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

5. Microsoft Windows Font Library 输入验证错误漏洞

（CNNVD-202007-600）

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 Windows Font Library 中存在安全漏洞，该漏洞源于程序没有正确处理特制字体。远程攻击者可利用该漏洞执行代码。以下产品及版本受到影响：Microsoft Windows 7 SP1，Windows 8.1，Windows RT 8.1，Windows 10，Windows Server 2008 SP2，Windows Server 2008 R2 SP1，Windows Server 2012，Windows Server 2012 R2，Windows Server 2016，Windows Server 2019，Windows 10 1607 版本，Windows 10 1709 版本，Windows 10 1803 版本，Windows 10 1809 版本，Windows 10 1903 版本，Windows 10 1909 版本，Windows 10 2004 版本，Windows Server 1903 版本，Windows Server 1909 版本，Windows Server 2004 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://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1436

6. IBM Maximo Asset Management 信息泄露漏洞

（CNNVD-202007-1688）

IBM Maximo Asset Management 是美国 IBM 公司的一套综合性

资产生命周期和维护管理解决方案。该方案能够在一个平台上管理所有类型的资产，如设施、交通运输等，并对这些资产实现单点控制。

IBM Maximo Asset Management 7.6.0 版本和 7.6.1 版本中存在信息泄露漏洞，该漏洞源于程序没有正确处理 XML 外部实体。远程攻击者可利用该漏洞泄露敏感信息或消耗内存资源。

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/6253953

7. Adobe Download Manager 注入漏洞（CNNVD-202007-1018）

Adobe Download Manager 是美国奥多比（Adobe）公司的一款用于管理和下载 Adobe 产品的应用程序。

基于 Windows 平台的 Adobe Download Manager 2.0.0.518 版本中存在注入漏洞。攻击者可利用该漏洞执行任意代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://helpx.adobe.com/security/products/adm/apsb20-49.html

8. Google Chrome Developer Tools 资源管理错误漏洞（CNNVD-202007-993）

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。Developer Tools 是其中的一个开发者工具组件。

Google Chrome 84.0.4147.89 之前版本中的 Developer Tools 存在资源管理错误漏洞。攻击者可利用该漏洞执行任意代码或造成拒绝服务。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://chromereleases.googleblog.com/2020/07/stable-channel-update-for-desktop.html

二、接报漏洞情况

本月接报漏洞 8070 个，其中信息技术产品漏洞（通用型漏洞）314 个，网络信息系统漏洞（事件型漏洞）7756 个。

表 7 2020 年 7 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	3776
2	上海斗象信息科技有限公司	2847
3	长春嘉诚信息技术股份有限公司	393
4	北京华云安信息技术有限公司	218
5	内蒙古奥创科技有限公司	135
6	深圳开源互联网安全技术有限公司	83
7	北京天融信网络安全技术有限公司	75
8	西安四叶草信息技术有限公司	60
9	山东新潮信息技术有限公司	51
10	北京山石网科信息技术有限公司	46
11	北京数字观星科技有限公司	36
12	西安交大捷普有限公司	30
13	广州锦行网络科技有限公司	20
14	内蒙古洞明科技有限公司	20
15	杭州默安科技有限公司	19
16	远江盛邦(北京)网络安全科技股份有限公司	19

17	安徽长泰信息安全服务有限公司	18
18	北京顶象技术有限公司 洞见安全实验室	17
19	西安交大捷普网络科技有限公司	17
20	广东网安科技有限公司	14
21	国防科技大学	12
22	安徽华云网安信息技术有限公司	10
23	北京梆梆安全科技有限公司	10
24	北京赋云安运营科技有限公司	10
25	北京启明星辰信息安全技术有限公司	10
26	北京升鑫网络科技有限公司	10
27	四维创智（北京）科技发展有限公司	10
28	太极计算机股份有限公司	10
29	安徽锋刃信息科技有限公司	9
30	北京安华金和科技有限公司	9
31	北京威努特技术有限公司	9
32	个人	9
33	北京安帝科技有限公司 andisec 实验室	7
34	北京圣博润高新技术股份有限公司	7
35	上海安洵信息技术有限公司	7
36	北京智游网安科技有限公司	5
37	上海安识网络科技有限公司	5
38	北京长亭科技有限公司	3
39	杭州安恒信息技术股份有限公司	3

40	绿盟科技集团股份有限公司安全研究部	3
41	中国电信集团系统集成	3
42	上海匡创信息技术有限公司	2
43	美国印第安纳大学伯明顿分校，中国科学院信息工程研究所	2
44	锐捷网络股份有限公司	2
45	北京知道创宇信息技术有限公司	1
46	北京星阑科技有限公司	1
47	山西轩辕信息安全技术有限公司	1
48	上海大学机电工程与自动化学院	1
49	上海上讯信息技术股份有限公司	1
50	新华三技术有限公司	1
51	浙江宇视科技有限公司	1
52	北京众安天下科技有限公司	1
53	重庆信息通信咨询设计院 安知团队	1
报送总计		8070

三、重大漏洞预警

3.1 微软多个安全漏洞的预警

近日，微软官方发布了多个安全漏洞的公告，包括多款 Microsoft 产品安全漏洞（CNNVD-202007-592、CVE-2020-1025）、Microsoft Windows Server DNS Server 安全漏洞（CNNVD-202007-864、CVE-2020-1350）、Microsoft Windows Graphics Device Interface 安全漏洞（CNNVD-202007-601、CVE-2020-1435）等多个漏洞。成功利用

上述漏洞的攻击者可以在目标系统上执行任意代码、获取用户数据，提升权限等。微软多个产品和系统受漏洞影响。目前，微软官方已经发布漏洞修复补丁，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

2020 年 7 月 14 日，微软发布了 2020 年 7 月份安全更新，共 123 个漏洞的补丁程序，CNNVD 对这些漏洞进行了收录。本次更新涵盖了 Windows 操作系统、IE/Edge 浏览器、ChakraCore、Visual Studio、.Net 框架、Azure DevOps、Office 及 Office 服务等多个 Windows 平台下应用软件和组件。微软多个产品和系统版本受漏洞影响，具体影响范围可访问 https://portal.msrc.microsoft.com/zh-cn/security-guidance 查询，其中部分重要漏洞详情如下：

1、多款 Microsoft 产品安全漏洞（CNNVD-202007-592、CVE-2020-1025）

漏洞简介：当 Microsoft SharePoint Server 和 Skype for Business Server 不正确地处理 OAuth 令牌验证时，存在特权提升漏洞。成功利用此漏洞的攻击者可以绕过身份验证并实现不正当访问。

2、Microsoft Windows Server DNS Server 安全漏洞（CNNVD-202007-864、CVE-2020-1350）

漏洞简介：当 Windows 域名系统服务器无法正确处理请求时，存在远程代码执行漏洞。成功利用此漏洞的攻击者可以在本地系统帐

户的上下文中运行任意代码。配置为 DNS 服务器的 Windows 服务器会受到此漏洞影响。

3、Microsoft Windows 和 Windows Server 安全漏洞（CNNVD-202007-612、CVE-2020-1421）

漏洞简介： 如果处理了 .LNK 文件，则 Microsoft Windows 中存在一个远程代码执行漏洞。成功利用此漏洞的攻击者可能会获得与本地用户相同的用户权限。与拥有管理用户权限的用户相比，帐户被配置为拥有较少系统用户权限的用户受到的影响更小。

4、Microsoft Windows 和 Windows Server 安全漏洞（CNNVD-202007-600、CVE-2020-1436）

漏洞简介：当 Windows 字体库不正确地处理经特殊设计的字体时，存在远程代码执行漏洞。对于除 Windows 10 之外的所有系统，成功利用此漏洞的攻击者可以远程执行代码。对于 Windows 10 系统，成功利用此漏洞的攻击者可以利用受限的特权和功能在 AppContainer 沙盒上下文中执行代码。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。

5、Microsoft Windows Graphics 安全漏洞（CNNVD-202004-2138、CVE-2020-1408）（CNNVD-202007-619、CVE-2020-1412）

漏洞简介：当 Windows 字体库不正确地处理经特殊设计的嵌入字体时，存在远程代码执行漏洞。成功利用此漏洞的攻击者可以控制受影响的系统。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。与拥有管理用户权限的用户相比，

帐户被配置为拥有较少系统用户权限的用户受到的影响更小。

6、Microsoft Word 安全漏洞(CNNVD-202007-690、CVE-2020-1447)（CNNVD-202007-712、CVE-2020-1446）

漏洞简介：当 Microsoft Word 软件无法正确处理内存中的对象时，会触发远程代码执行漏洞。成功利用此漏洞的攻击者可以使用经特殊设计的文件在当前用户的安全上下文中执行操作。例如，文件可以代表登录用户使用与当前用户相同的权限执行操作。

7、Microsoft Windows 和 Windows Server 安全漏洞(CNNVD-202007-793、CVE-2020-1355)

漏洞简介：当 Windows 字体驱动程序主机不正确地处理内存时，存在远程代码执行漏洞。成功利用此漏洞的攻击者可以在受害者系统上获得执行权。

8、Microsoft Windows Jet Database Engine 安全漏洞(CNNVD-202007-628、CVE-2020-1401)

漏洞简介：当 Windows Jet 数据库引擎不正确地处理内存中的对象时，存在远程代码执行漏洞。成功利用此漏洞的攻击者可以在受害者系统上执行任意代码。攻击者可以通过诱使受害者打开经特殊设计的文件来利用此漏洞。

9、Microsoft SharePoint 安全漏洞(CNNVD-202007-590、CVE-2020-1444)

漏洞简介：Microsoft SharePoint 软件分析经特殊设计的电子邮件的方式中存在远程代码执行漏洞。成功利用此漏洞的攻击者可以在

系统用户的上下文中运行任意代码。然后，攻击者可以安装程序；查看、更改、添加或删除数据。

10、Microsoft Windows Codecs Library 安全漏洞(CNNVD-202006-1889、CVE-2020-1457)

漏洞简介：当 Microsoft Windows Codecs 库处理内存中的对象时，存在远程代码执行漏洞。成功利用此漏洞的攻击者可以执行任意代码。攻击者需要程序处理经特殊设计的文件才能利用此漏洞。

11、Microsoft Windows Graphics Device Interface 安全漏洞(CNNVD-202007-601、CVE-2020-1435)

漏洞简介：Windows 图形设备接口 (GDI) 处理内存中对象的方式中存在远程代码执行漏洞。成功利用此漏洞的攻击者可能会控制受影响的系统。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。与拥有管理用户权限的用户相比，帐户被配置为拥有较少系统用户权限的用户受到的影响更小。

修复建议

目前，微软官方已经发布补丁修复了上述漏洞，建议用户及时确认漏洞影响，尽快采取修补措施。微软官方链接地址如下：

序号	漏洞名称	官方链接
1	多款 Microsoft 产品安全漏洞（CNNVD-202007-592、CVE-2020-1025）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1025
2	Microsoft Windows Server DNS Server 安全漏洞（CNNVD-202007-864、CVE-2020-1350）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1350
3	Microsoft Windows 和 Windows Server 安全漏洞（CNNVD-202007-612、CVE-2020-1421）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1421
4	Microsoft Windows 和 Windows Server 安全漏洞	https://portal.msrc.microsoft.com/zh-CN/sec

	（CNNVD-202007-600、CVE-2020-1436）	urity-guidance/advisory/CVE-2020-1436
5	Microsoft Windows Graphics 安全漏洞（CNNVD-202004-2138 、 CVE-2020-1408 ）（CNNVD-202007-619、CVE-2020-1412）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1408 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1412
6	Microsoft Word 安全漏洞(CNNVD-202007-690、CVE-2020-1447) （ CNNVD-202007-712 、CVE-2020-1446）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1447 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1446
7	Microsoft Windows 和 Windows Server 安全漏洞(CNNVD-202007-793、CVE-2020-1355)	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1355
8	Microsoft Windows Jet Database Engine 安全漏洞(CNNVD-202007-628、CVE-2020-1401)	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1401
9	Microsoft SharePoint 安全漏洞(CNNVD-202007-590、CVE-2020-1444)	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1444
10	Microsoft Windows Codecs Library 安全漏洞(CNNVD-202006-1889、CVE-2020-1457)	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1457
11	Microsoft Windows Graphics Device Interface 安全漏洞(CNNVD-202007-601、CVE-2020-1435)	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1435

3.2 Oracle WebLogic 多个安全漏洞的预警

近日，Oracle 发布了多个安全漏洞的公告，包括 Oracle Fusion Middleware WebLogic Server 安全漏（CNNVD-202007-825、 CVE-2020-14625）、Oracle Fusion Middleware WebLogic Server 安全漏洞（CNNVD-202007-823、CVE-2020-14644）、Oracle Fusion Middleware WebLogic Server Core 组件安全漏洞（CNNVD-202007-820、CVE-2020-14645）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 7 月 14 日，Oracle 发布了大量安全补丁，共 443 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：

序号	漏洞名称	漏洞编号	影响版本
1	Oracle Fusion Middleware WebLogic Server 安全漏	CNNVD-202007-825 CVE-2020-14625	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 Fusion Middleware WebLogic Server 安全漏洞	CNNVD-202007-823 CVE-2020-14644	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 Fusion Middleware WebLogic Server Core 组件安全漏洞	CNNVD-202007-820 CVE-2020-14645	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
4	Oracle Fusion Middleware WebLogic Server 安全漏洞	CNNVD-202007-818 CVE-2020-14687	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