

北京师范大学网络信息安全通告

2021 年 6 月报告

北京师范大学信息网络中心

2021 年 7 月

目录

| | |
|-------------------------------------|----|
| 漏洞态势 | 1 |
| 1. 公开漏洞情况..... | 2 |
| 1.1. 漏洞增长概况..... | 2 |
| 1.2. 漏洞分布情况..... | 3 |
| 1.2.1. 漏洞厂商分布 | 3 |
| 1.2.2. 漏洞产品分布 | 3 |
| 1.2.3. 漏洞类型分布 | 4 |
| 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 | 7 |
| 1.4.1. 超危漏洞实例 | 7 |
| 1.4.2. 高危漏洞实例 | 13 |
| 2. 漏洞平台推送情况..... | 25 |
| 3. 接报漏洞情况 | 25 |
| 4. 重大漏洞预警..... | 28 |
| 4.1. 微软多个安全漏洞的预警..... | 28 |
| 4.2. 用友NC BeanShell远程代码执行漏洞的预警..... | 34 |

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，2021年6月份新增安全漏洞共1535个，从厂商分布来看，Intel公司产品的漏洞数量最多，共发布73个；从漏洞类型来看，缓冲区错误类的漏洞占比最大，达到12.90%。本月新增漏洞中，超危漏洞170个、高危漏洞619个、中危漏洞691个、低危漏洞55个，相应修复率分别为79.41%、78.84%、83.94%以及83.64%。合计1249个漏洞已有修复补丁发布，本月整体修复率81.37%。

截至2021年6月30日，CNNVD采集漏洞总量已达165363个。

1.1 漏洞增长概况

2021年6月新增安全漏洞1535个，与上月（1682个）相比减少了8.74%。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1607个。

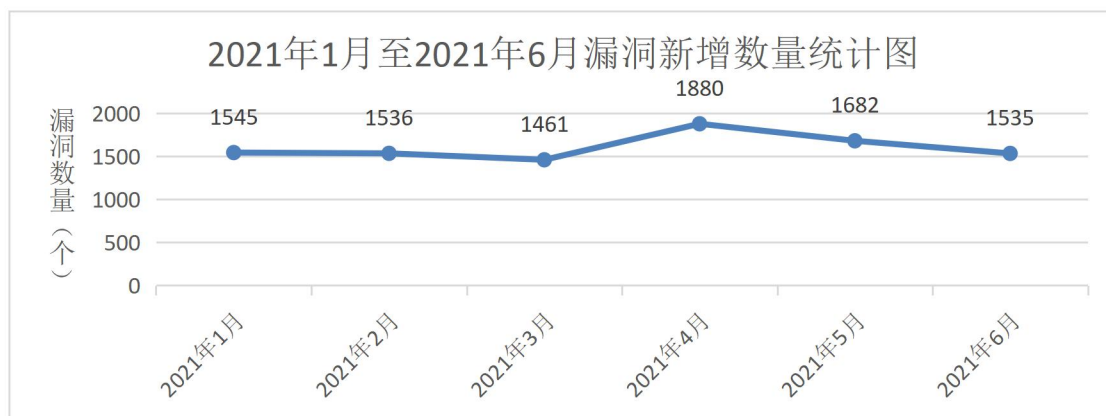


图1 2021年1月至6月漏洞新增数量统计图

1.2 漏洞分布情况

1.2.1 漏洞厂商分布

2021年6月厂商漏洞数量分布情况如表1所示，Intel公司漏洞达到73个，占本月漏洞总量的4.76%。

表1 2021年6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(个) | 所占比例 |
|----|---------------|---------|-------|
| 1 | Intel | 73 | 4.76% |
| 2 | WordPress 基金会 | 65 | 4.23% |
| 3 | Microsoft | 55 | 3.58% |
| 4 | IBM | 49 | 3.19% |
| 5 | Huawei | 45 | 2.93% |
| 6 | Adobe | 43 | 2.80% |
| 7 | Samsung | 43 | 2.80% |
| 8 | SAP | 39 | 2.54% |
| 9 | Google | 33 | 2.15% |
| 10 | Cisco | 27 | 1.76% |

1.2.2 漏洞产品分布

2021年6月主流操作系统的漏洞统计情况如表2所示。本月Windows 10漏洞数量最多，共25个，占主流操作系统漏洞总量的12.76%，排名第一。

表2 2021年6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 | 25 |
| 2 | Windows Server 2019 | 23 |
| 3 | Windows Server 2016 | 19 |
| 4 | Windows Server 2012 | 18 |
| 5 | Windows Server 2012 R2 | 18 |
| 6 | Windows 8.1 | 18 |
| 7 | Windows Rt 8.1 | 18 |

| | | |
|----|------------------------|----|
| 8 | Windows Server 2008 | 13 |
| 9 | Windows Server 2008 R2 | 13 |
| 10 | Windows 7 | 13 |
| 11 | Android | 13 |
| 12 | Linux Kernel | 5 |

1.2.3 漏洞类型分布

2021年6月份发布的漏洞类型分布如表3所示，其中缓冲区错误类漏洞所占比例最大，约为12.90%。

表3 2021年6月漏洞类型统计表

| 序号 | 漏洞类型 | 漏洞数量(个) | 所占比例 |
|----|-------------|---------|--------|
| 1 | 缓冲区错误 | 198 | 12.90% |
| 2 | 跨站脚本 | 193 | 12.57% |
| 3 | 输入验证错误 | 117 | 7.62% |
| 4 | 代码问题 | 114 | 7.43% |
| 5 | 资源管理错误 | 83 | 5.41% |
| 6 | 信息泄露 | 69 | 4.50% |
| 7 | SQL注入 | 64 | 4.17% |
| 8 | 访问控制错误 | 48 | 3.13% |
| 9 | 授权问题 | 39 | 2.54% |
| 10 | 权限许可和访问控制问题 | 30 | 1.95% |
| 11 | 代码注入 | 26 | 1.69% |
| 12 | 路径遍历 | 25 | 1.63% |
| 13 | 跨站请求伪造 | 21 | 1.37% |
| 14 | 命令注入 | 20 | 1.30% |
| 15 | 信任管理问题 | 19 | 1.24% |
| 16 | 操作系统命令注入 | 15 | 0.98% |
| 17 | 注入 | 11 | 0.72% |
| 18 | 竞争条件问题 | 9 | 0.59% |
| 19 | 数据伪造问题 | 9 | 0.59% |
| 20 | 处理逻辑错误 | 9 | 0.59% |
| 21 | 安全特征问题 | 8 | 0.52% |
| 22 | 加密问题 | 8 | 0.52% |
| 23 | 日志信息泄露 | 7 | 0.46% |
| 24 | 数字错误 | 3 | 0.20% |
| 25 | 环境问题 | 3 | 0.20% |
| 26 | 后置链接 | 2 | 0.13% |
| 27 | 配置错误 | 2 | 0.13% |

| | | | |
|----|----------|-----|--------|
| 28 | 参数注入 | 1 | 0.07% |
| 29 | 格式化字符串错误 | 1 | 0.07% |
| 30 | 默认配置问题 | 1 | 0.07% |
| 31 | 调试信息泄露 | 0 | 0.00% |
| 32 | 其他 | 380 | 24.76% |

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。2021年6月漏洞危害等级分布如图2所示，其中超危漏洞170条，占本月漏洞总数的11.07%。

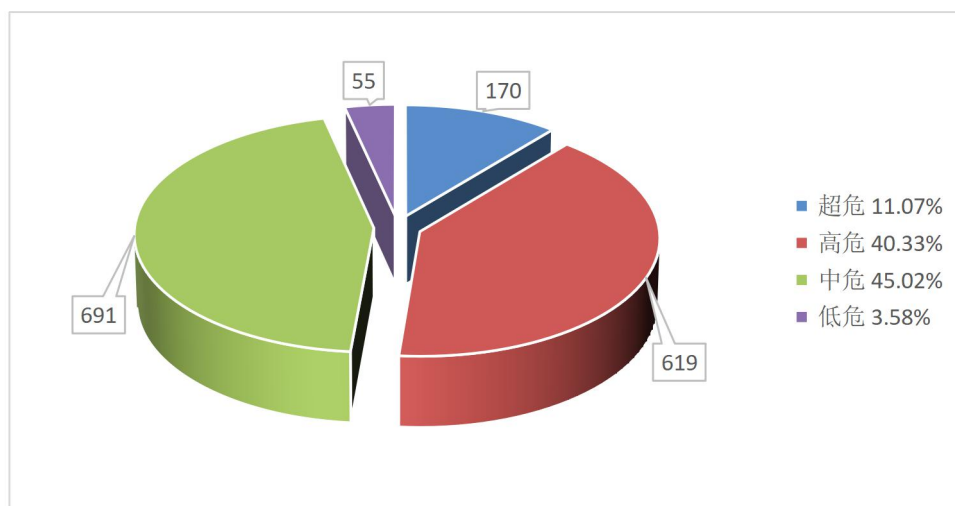


图2 2021年6月漏洞危害等级分布

1.3 漏洞修复情况

1.3.1 整体修复情况

2021年6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83.94%，高危漏洞修复率最低，比例为78.84%。

总体来看，本月整体修复率，由上月的87.31%下降至本月的81.37%。

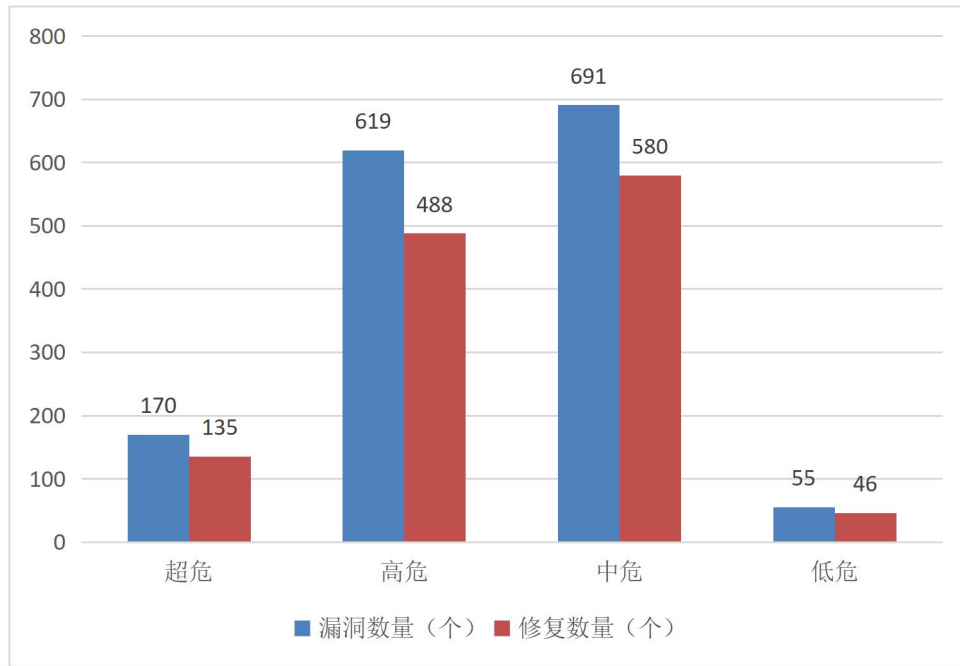


图 3 2021 年 6 月漏洞修复数量统计

1.3.2 厂商修复情况

2021 年 6 月漏洞修复情况按漏洞数量前十厂商进行统计，其中 Intel、WordPress 基金会、Microsoft 等十个厂商共 472 条漏洞，占本月漏洞总数的 30.75%，漏洞修复率为 91.31%，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 Microsoft、Samsung、SAP 等公司本月漏洞修复率均为 100%，共 431 条漏洞已全部修复。

表 4 2021 年 6 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 | Intel | 73 | 67 | 91.78% |
| 2 | WordPress 基金会 | 65 | 64 | 98.46% |
| 3 | Microsoft | 55 | 55 | 100.00% |
| 4 | IBM | 49 | 44 | 89.80% |
| 5 | Huawei | 45 | 43 | 95.56% |
| 6 | Adobe | 43 | 29 | 67.44% |
| 7 | Samsung | 43 | 43 | 100.00% |
| 8 | SAP | 39 | 39 | 100.00% |
| 9 | Google | 33 | 30 | 90.91% |

| | | | | |
|----|-------|----|----|--------|
| 10 | Cisco | 27 | 17 | 62.96% |
|----|-------|----|----|--------|

1.4 重要漏洞实例

1.4.1 超危漏洞实例

本月超危漏洞共 170 个，其中重要漏洞实例如表 5 所示。

表 5 2021 年 6 月超危漏洞实例

| 序号 | 漏洞类型 | 厂商 | CNNVD 编号 | 漏洞实例 |
|-------------------|-------------------|--------------------------|-------------------|--|
| 1 | SQL 注入 | Chamilo 协会 | CNNVD-202106-1913 | Synology Photo Station SQL 注入漏洞 (CNNVD-202106-114) |
| | | Desdev | CNNVD-202106-1321 | |
| | | Fangfa | CNNVD-202106-201 | |
| | | Fidelis | CNNVD-202106-1727 | |
| | | In4Velocity | CNNVD-202106-028 | |
| | | Moldeo | CNNVD-202106-1695 | |
| | | SourceCodester | CNNVD-202106-1269 | |
| | | Synology | CNNVD-202106-114 | |
| | | | CNNVD-202106-070 | |
| | | WordPress 基金会 | CNNVD-202106-1509 | |
| | | | CNNVD-202106-048 | |
| | | primion Technology AG | CNNVD-202106-1423 | |
| | | 个人开发者 | CNNVD-202106-1334 | |
| | | | CNNVD-202106-1333 | |
| | | | CNNVD-202106-1335 | |
| | | | CNNVD-202106-1683 | |
| | | | CNNVD-202106-1632 | |
| | | | CNNVD-202106-1713 | |
| | | | CNNVD-202106-1329 | |
| | | | CNNVD-202106-1716 | |
| CNNVD-202106-1337 | | | | |
| CNNVD-202106-1903 | | | | |
| 迅易科技 | CNNVD-202106-1351 | | | |
| | CNNVD-202106-1338 | | | |
| | CNNVD-202106-1336 | | | |
| | CNNVD-202106-1344 | | | |
| | CNNVD-202106-1358 | | | |
| 2 | 代码问题 | Apache 基金会 | CNNVD-202106-056 | Apache Dubbo 代码问题漏洞 |
| | | | CNNVD-202106-064 | |
| | | | CNNVD-202106-1293 | |
| | | BloofoxCms | CNNVD-202106-1326 | |

| | | | | |
|-------------------|-------------------|----------------------------|-------------------|--|
| | | ConnectWise | CNNVD-202106-1526 | (CNNVD-202106-056) |
| | | Fangfa | CNNVD-202106-202 | |
| | | GitLab | CNNVD-202106-956 | |
| | | IBM | CNNVD-202106-919 | |
| | | Jenkins | CNNVD-202106-1406 | |
| | | Mcafee | CNNVD-202106-165 | |
| | | Mojang | CNNVD-202106-226 | |
| | | Open Source Matters | CNNVD-202106-1530 | |
| | | Raonwiz | CNNVD-202106-1274 | |
| | | Rockwell Automation | CNNVD-202106-523 | |
| | | Singularity 团队 | CNNVD-202106-1276 | |
| | | Synology | CNNVD-202106-072 | |
| | | Textpattern 团队 | CNNVD-202106-1499 | |
| | | Vembu | CNNVD-202106-611 | |
| | | WordPress 基金会 | CNNVD-202106-1518 | |
| | | | CNNVD-202106-1389 | |
| | | | CNNVD-202106-151 | |
| | | Zhongbang | CNNVD-202106-1679 | |
| pandorafms | CNNVD-202106-1735 | | | |
| 个人开发者 | CNNVD-202106-1205 | | | |
| | CNNVD-202106-1232 | | | |
| | CNNVD-202106-1689 | | | |
| | CNNVD-202106-1691 | | | |
| 3 | 授权问题 | Automation Direct | CNNVD-202106-1280 | VMware Carbon Black App Control 授权问题漏洞 (CNNVD-202106-1545) |
| | | CHIYU | CNNVD-202106-214 | |
| | | D-link | CNNVD-202106-1694 | |
| | | Palo Alto | CNNVD-202106-1541 | |
| | | SAP | CNNVD-202106-470 | |
| | | Schneider-electric | CNNVD-202106-1009 | |
| | | Silverstripe | CNNVD-202106-599 | |
| | | Vmware | CNNVD-202106-1545 | |
| | | ZOHO | CNNVD-202106-1725 | |
| 个人开发者 | CNNVD-202106-1363 | | | |
| 4 | 操作系统命令注入 | s21sec | CNNVD-202106-727 | Circutor SGE-PLC1000 操作系统命令注入漏洞 (CNNVD-202106-727) |
| | | 个人开发者 | CNNVD-202106-1547 | |
| | | | CNNVD-202106-747 | |
| 5 | 缓冲区错误 | Accusoft | CNNVD-202106-091 | Matrix libm 缓冲区错误漏洞 (CNNVD-202106-1343) |
| | | Apache 基金会 | CNNVD-202106-216 | |
| | | Arch Linux 社区 | CNNVD-202106-751 | |
| | | Eipstackgroup | CNNVD-202106-1361 | |
| | | JerryScript | CNNVD-202106-840 | |

| | | | | |
|-------|-------------------|---------------------------|-------------------|--|
| | | | CNNVD-202106-837 | |
| | | | CNNVD-202106-834 | |
| | | | CNNVD-202106-842 | |
| | | Matrix | CNNVD-202106-1343 | |
| | | Mmemed | CNNVD-202106-107 | |
| | | Mobile Viewpoint | CNNVD-202106-180 | |
| | | Samsung | CNNVD-202106-920 | |
| | | WIBU | CNNVD-202106-1297 | |
| | | 个人开发者 | CNNVD-202106-1426 | |
| | | | CNNVD-202106-1427 | |
| | | | CNNVD-202106-1428 | |
| | | | CNNVD-202106-346 | |
| 6 | 访问控制 错误 | Advantech | CNNVD-202106-259 | Advantech Iview 访问控制错误漏洞 (CNNVD-202106-259) |
| | | Bosch | CNNVD-202106-738 | |
| | | Symantec | CNNVD-202106-1968 | |
| 7 | 资源管理 错误 | Facebook | CNNVD-202106-1283 | Facebook Hermes 资源管理错误漏洞 (CNNVD-202106-1283) |
| | | JerryScript | CNNVD-202106-825 | |
| | | Synology | CNNVD-202106-1617 | |
| | | 个人开发者 | CNNVD-202106-1733 | |
| | | | CNNVD-202106-200 | |
| 8 | 输入验证 错误 | Accusoft | CNNVD-202106-071 | Schneider Electric PowerLogic 输入验证错误漏洞 (CNNVD-202106-984) |
| | | | CNNVD-202106-076 | |
| | | | CNNVD-202106-142 | |
| | | Bosch | CNNVD-202106-742 | |
| | | Eclipse 基金会 | CNNVD-202106-1740 | |
| | | Ethereum | CNNVD-202106-1701 | |
| | | Huawei | CNNVD-202106-243 | |
| | | Mobile Viewpoint | CNNVD-202106-178 | |
| | | Nginx | CNNVD-202106-378 | |
| | | Qualcomm | CNNVD-202106-383 | |
| | | Samsung | CNNVD-202106-926 | |
| | | Schneider Electric | CNNVD-202106-984 | |
| | | | CNNVD-202106-992 | |
| | | | CNNVD-202106-1007 | |
| | | Siemens | CNNVD-202106-1272 | |
| 个人开发者 | CNNVD-202106-1887 | | | |

1. Synology Photo Station SQL 注入漏洞 (CNNVD-202106-114)

Synology Photo Station 是中国台湾群晖科技 (Synology) 公司的一套用于在互联网上共享图片、视频和博客的解决方案。

Synology Photo Station 6.8.14-3500 之前版本存在 SQL 注入漏洞，攻击者可利用该漏洞用户通过未指定的向量执行任意 SQL 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://www.synology.com/security/advisory/Synology_SA_20_20

2. Apache Dubbo 代码问题漏洞（CNNVD-202106-056）

Apache Dubbo 是美国阿帕奇（Apache）基金会的一款基于 Java 的轻量级 RPC（远程过程调用）框架。该产品提供了基于接口的远程呼叫、容错和负载均衡以及自动服务注册和发现等功能。

Apache Dubbo 2.7.8 和 2.6.9 之前版本存在代码问题漏洞，该漏洞源于攻击者利用该漏洞可以通过篡改字节前序标志(也就是不遵循服务器的指令)来选择提供者将使用哪个序列化 id。

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/r99ef7fa35585d3a68762de07e8d2b2bc48b8fa669a03e8d84b9673f3%40%3Cdev.dubbo.apache.org%3E>

3. VMware Carbon Black App Control 授权问题漏洞（CNNVD-202106-1545）

Vmware VMware Carbon Black App Control 是美国 Vmware 公司的一款应用控制产品。用于锁定服务器和关键系统，防止不必要的更改。

VMware Carbon Black App Control 8.0、8.1、8.5.8 之前的 8.5、8.6.2 之前的 8.6 存在授权问题漏洞。该漏洞允许具有 VMware Carbon Black App Control 管理服务器网络访问权的攻击者获得对产品的管

理访问权，而不需要进行身份验证。

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-2021-0012.html>

4. Circutor SGE-PLC1000 操作系统命令注入漏洞 (CNNVD-202106-727)

Circutor SGE-PLC1000 是一个智能计量系统的设备。主要功能是通过 CIRWATT 电表或其他采用 PRIME 技术的电表管理市电。

SGE-PLC1000 中存在操作系统命令注入漏洞，该漏洞源于该设备不能正确地处理一些请求，远程攻击者可利用该漏洞以最大的权限向操作系统注入代码。以下产品及型号会受到影响：SGE-PLC1000 0.9.2b 固件版本。

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.s21sec.com/>

5. Matrix libm 缓冲区错误漏洞 (CNNVD-202106-1343)

Matrix libolm 是一个加密库。

Matrix libm 存在安全漏洞，该漏洞源于在 3.2.3 之前版本的 Matrix libm 允许一个恶意的 Matrix 主服务器崩溃一个客户端(当它试图从主服务器检索一个 Olm 加密的房间密钥备份)，因为 Olm pk 解密有一个基于堆栈的缓冲区溢出。攻击者可利用该漏洞远程代码执行。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

<https://matrix.org/blog/2021/06/14/adventures-in-fuzzing-libolm>

6. Advantech Iview 访问控制错误漏洞（CNNVD-202106-259）

Advantech Iview 是中国 Advantech 公司的一个基于简单网络协议（SNMP）来对 B + B SmartWorx 设备进行管理的软件。

IView 5.7.03.6182 版本存在访问控制错误漏洞，该漏洞源于程序缺少身份验证，受影响的产品配置容易受到攻击，这可能会使攻击者利用该漏洞更改配置并执行任意代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

<https://advantech-bb.com/product/iview-snmp-management-software/>

7. Facebook Hermes 资源管理错误漏洞

Facebook Hermes 是美国 Facebook 公司的一个 JavaScript 引擎。该引擎针对 React Native 应用，去提高移动客户端应用 App 的性能，但是对浏览器 & Node.js 等服务端基础架构并不适用。

Hermes 中存在资源管理错误漏洞，该漏洞源于未对输入数据进行安全性检查，攻击者可通过构造特殊的 javascript 执行代码。以下产品及版本受到影响：`hermes d86e185e485b6330216dee8e854455c694e3a36e` 之前版本受到影响。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

<https://github.com/facebook/hermes/commit/d86e185e485b6330216dee8e854455c694e3a36e>

8. Schneider Electric PowerLogic 输入验证错误漏洞（CNNVD-202106-984）

Schneider Electric PowerLogic 是法国施耐德电气（Schneider Electric）公司的一个工控设备。提供提高功率因数来提高电源质量，排除电源故障，从而保护网络、装置和操作人员。

PowerLogic EGX100 和 EGX100 存在输入验证错误漏洞，该漏洞源于不正确的输入验证存在于 PowerLogic EGX100(版本 3.0.0 和更新) 和 PowerLogic EGX300(所有版本)，攻击者可利用该漏洞导致拒绝服务或通过特殊制作的 HTTP 包远程代码执行。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

http://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-159-03

1.4.2 高危漏洞实例

本月高危漏洞共 619 个，其中重点漏洞实例如表 6 所示。

表 6 2021 年 6 月高危漏洞实例

| 序号 | 漏洞类型 | 厂商 | CNNVD 编号 | 漏洞实例 |
|--------------------------|------------------|--------------------|-------------------|---|
| 1 | SQL 注入 | Advantech | CNNVD-202106-250 | Connectwise ConnectWise Automate SQL 注入漏洞 (CNNVD-202106-1402) |
| | | Connectwise | CNNVD-202106-1402 | |
| | | Fastspot | CNNVD-202106-079 | |
| | | PHPGurukul | CNNVD-202106-1575 | |
| | | | CNNVD-202106-1584 | |
| | | | CNNVD-202106-1577 | |
| | | | CNNVD-202106-1585 | |
| | | | CNNVD-202106-1576 | |
| | | | CNNVD-202106-1580 | |
| | | | CNNVD-202106-1582 | |
| | | | CNNVD-202106-1581 | |
| | | | CNNVD-202106-1587 | |
| | | | CNNVD-202106-1586 | |
| | | CNNVD-202106-1583 | | |
| Progress Software | CNNVD-202106-758 | | | |

| | | | | | | | |
|---------------------|-------------------|------------------------|-------------------|--|-------------------|-------------------|---|
| | | Sourcecodester | CNNVD-202106-193 | | | | |
| | | Synology | CNNVD-202106-116 | | | | |
| | | Trace Financial | CNNVD-202106-810 | | | | |
| | | | CNNVD-202106-813 | | | | |
| | | WordPress 基金会 | CNNVD-202106-1211 | | | | |
| | | | CNNVD-202106-1215 | | | | |
| | | | CNNVD-202106-389 | | | | |
| | | 个人开发者 | CNNVD-202106-395 | | | | |
| | | | CNNVD-202106-1622 | | | | |
| | | | CNNVD-202106-1519 | | | | |
| | | | CNNVD-202106-1535 | | | | |
| | | | CNNVD-202106-191 | | | | |
| | | | CNNVD-202106-1693 | | | | |
| | | 2 | 代码问题 | | Adobe | CNNVD-202106-1534 | Microsoft Office SharePoint 代码问题漏洞 (CNNVD-202106-492) |
| | | | | | | CNNVD-202106-1884 | |
| | | | | | Apache 基金会 | CNNVD-202106-662 | |
| | | | | | | CNNVD-202106-166 | |
| | | | | | | CNNVD-202106-212 | |
| | | | | | Cisco | CNNVD-202106-139 | |
| | | | | | | CNNVD-202106-1299 | |
| Django 基金会 | CNNVD-202106-188 | | | | | | |
| Epam Systems | CNNVD-202106-144 | | | | | | |
| F5 | CNNVD-202106-1636 | | | | | | |
| Freebsd 基金会 | CNNVD-202106-129 | | | | | | |
| GitLab | CNNVD-202106-1564 | | | | | | |
| HashiCorp | CNNVD-202106-588 | | | | | | |
| Huawei | CNNVD-202106-227 | | | | | | |
| Intel | CNNVD-202106-1441 | | | | | | |
| | CNNVD-202106-620 | | | | | | |
| | CNNVD-202106-709 | | | | | | |
| | CNNVD-202106-734 | | | | | | |
| | CNNVD-202106-693 | | | | | | |
| JerryScript | CNNVD-202106-689 | | | | | | |
| | CNNVD-202106-713 | | | | | | |
| | CNNVD-202106-827 | | | | | | |
| | CNNVD-202106-828 | | | | | | |
| Mcafee | CNNVD-202106-830 | | | | | | |
| | CNNVD-202106-829 | | | | | | |
| Microsoft | CNNVD-202106-826 | | | | | | |
| | CNNVD-202106-768 | | | | | | |
| Nagios | CNNVD-202106-175 | | | | | | |
| | | Microsoft | CNNVD-202106-492 | | | | |
| | | Nagios | CNNVD-202106-424 | | | | |

| | | | | |
|--------------------|-------------------|------------------------------|-------------------|--|
| | | Open Design Alliance | CNNVD-202106-687 | |
| | | OpenVPN | CNNVD-202106-352 | |
| | | Palo Alto Networks | CNNVD-202106-679 | |
| | | Synology | CNNVD-202106-061 | |
| | | | CNNVD-202106-073 | |
| | | TeamViewer | CNNVD-202106-1318 | |
| | | The Trusted Domain 项目 | CNNVD-202106-809 | |
| | | ThinkJS 组织 | CNNVD-202106-2004 | |
| | | Wordpress 基金会 | CNNVD-202106-039 | |
| | | ZOLL | CNNVD-202106-838 | |
| | | 个人开发者 | CNNVD-202106-678 | |
| | | | CNNVD-202106-1323 | |
| | | | CNNVD-202106-033 | |
| | | | CNNVD-202106-380 | |
| | | | CNNVD-202106-1279 | |
| | | | CNNVD-202106-1533 | |
| | | | CNNVD-202106-1623 | |
| | | | CNNVD-202106-239 | |
| | | | CNNVD-202106-1385 | |
| | | | CNNVD-202106-1925 | |
| | | | CNNVD-202106-241 | |
| CNNVD-202106-360 | | | | |
| CNNVD-202106-249 | | | | |
| CNNVD-202106-1356 | | | | |
| CNNVD-202106-1342 | | | | |
| 3 | 授权问题 | Circutor | CNNVD-202106-728 | Intel Virtualization 授权问题漏洞 (CNNVD-202106-630) |
| | | Cisco | CNNVD-202106-124 | |
| | | | CNNVD-202106-125 | |
| | | | CNNVD-202106-1307 | |
| | | Huawei | CNNVD-202106-235 | |
| | | Intel | CNNVD-202106-630 | |
| | | Open Source Matters | CNNVD-202106-1531 | |
| | | Samsung | CNNVD-202106-950 | |
| | | | CNNVD-202106-918 | |
| | | Sensio Labs | CNNVD-202106-1366 | |
| | | Shopware | CNNVD-202106-1705 | |
| Weidmueller | CNNVD-202106-1754 | | | |
| 个人开发者 | CNNVD-202106-750 | | | |

| | | | | |
|-------------------|------------------|---------------------|-------------------|--|
| 4 | 操作系统 命令注入 | Cisco | CNNVD-202106-123 | Fortinet FortiWeb 操作系统 命令注入漏洞 (CNNVD-202106-013) |
| | | Fidelis | CNNVD-202106-1726 | |
| | | Fortinet | CNNVD-202106-013 | |
| | | Hitachi | CNNVD-202106-1404 | |
| | | Weidmueller | CNNVD-202106-1747 | |
| | | | CNNVD-202106-1762 | |
| | | | CNNVD-202106-1749 | |
| | | | CNNVD-202106-1750 | |
| | | myq-solution | CNNVD-202106-1478 | |
| | | 个人开发者 | CNNVD-202106-1881 | |
| CNNVD-202106-748 | | | | |
| CNNVD-202106-1544 | | | | |
| 5 | 缓冲区错 误 | Accusoft | CNNVD-202106-097 | Adobe After Effects 缓冲区错误漏洞 (CNNVD-202106-646) |
| | | | CNNVD-202106-085 | |
| | | Adobe | CNNVD-202106-646 | |
| | | | CNNVD-202106-648 | |
| | | | CNNVD-202106-486 | |
| | | | CNNVD-202106-549 | |
| | | | CNNVD-202106-485 | |
| | | | CNNVD-202106-664 | |
| | | | CNNVD-202106-667 | |
| | | | CNNVD-202106-647 | |
| | | Advantech | CNNVD-202106-1539 | |
| | | | CNNVD-202106-1538 | |
| | | | CNNVD-202106-1537 | |
| | | Apache 基金会 | CNNVD-202106-150 | |
| | | | CNNVD-202106-1963 | |
| | | Apple | CNNVD-202106-1243 | |
| | | Autodesk | CNNVD-202106-1561 | |
| | | | CNNVD-202106-1649 | |
| | | | CNNVD-202106-1568 | |
| | | | CNNVD-202106-1579 | |
| | | | CNNVD-202106-1598 | |
| | | Cisco | CNNVD-202106-119 | |
| | | | CNNVD-202106-117 | |
| | | | CNNVD-202106-118 | |
| | | D-Link | CNNVD-202106-1352 | |
| | | | CNNVD-202106-1350 | |
| | | Dell | CNNVD-202106-1666 | |
| CNNVD-202106-1661 | | | | |
| CNNVD-202106-1656 | | | | |
| FFmpeg | CNNVD-202106-106 | | | |
| Google | CNNVD-202106-432 | | | |

| | | | | |
|--|--|-----------------------------|-------------------|--|
| | | | CNNVD-202106-762 | |
| | | | CNNVD-202106-429 | |
| | | Huawei | CNNVD-202106-258 | |
| | | IBM | CNNVD-202106-1722 | |
| | | Intel | CNNVD-202106-696 | |
| | | | CNNVD-202106-699 | |
| | | | CNNVD-202106-695 | |
| | | | CNNVD-202106-636 | |
| | | JerryScript | CNNVD-202106-844 | |
| | | Libraw | CNNVD-202106-181 | |
| | | Linux 基金会 | CNNVD-202106-1390 | |
| | | | CNNVD-202106-1659 | |
| | | Mcafee | CNNVD-202106-676 | |
| | | Microsoft | CNNVD-202106-501 | |
| | | | CNNVD-202106-497 | |
| | | | CNNVD-202106-505 | |
| | | Mmemed | CNNVD-202106-098 | |
| | | Mozilla 基金会 | CNNVD-202106-006 | |
| | | | CNNVD-202106-1292 | |
| | | | CNNVD-202106-003 | |
| | | | CNNVD-202106-004 | |
| | | Nvidia | CNNVD-202106-1462 | |
| | | Open Design Alliance | CNNVD-202106-681 | |
| | | | CNNVD-202106-683 | |
| | | | CNNVD-202106-680 | |
| | | | CNNVD-202106-685 | |
| | | | CNNVD-202106-686 | |
| | | | CNNVD-202106-684 | |
| | | OpenText | CNNVD-202106-1258 | |
| | | | CNNVD-202106-148 | |
| | | | CNNVD-202106-391 | |
| | | | CNNVD-202106-1252 | |
| | | | CNNVD-202106-1256 | |
| | | | CNNVD-202106-1254 | |
| | | | CNNVD-202106-147 | |
| | | | CNNVD-202106-1257 | |
| | | | CNNVD-202106-1253 | |
| | | Opentext | CNNVD-202106-145 | |
| | | | CNNVD-202106-173 | |
| | | | CNNVD-202106-149 | |
| | | | CNNVD-202106-157 | |
| | | | CNNVD-202106-176 | |
| | | | CNNVD-202106-137 | |

| | | | | |
|--|--|---------------------------|-------------------|--|
| | | | CNNVD-202106-1259 | |
| | | | CNNVD-202106-141 | |
| | | | CNNVD-202106-162 | |
| | | | CNNVD-202106-159 | |
| | | | CNNVD-202106-138 | |
| | | | CNNVD-202106-153 | |
| | | | CNNVD-202106-161 | |
| | | | CNNVD-202106-152 | |
| | | Polaris Office | CNNVD-202106-593 | |
| | | PowerISO | CNNVD-202106-1922 | |
| | | QNAP Systems | CNNVD-202106-1196 | |
| | | Qualcomm | CNNVD-202106-381 | |
| | | | CNNVD-202106-384 | |
| | | RIOT | CNNVD-202106-1434 | |
| | | | CNNVD-202106-1431 | |
| | | | CNNVD-202106-1432 | |
| | | | CNNVD-202106-1430 | |
| | | Realtek | CNNVD-202106-358 | |
| | | | CNNVD-202106-355 | |
| | | Samsung | CNNVD-202106-932 | |
| | | Schneider Electric | CNNVD-202106-617 | |
| | | | CNNVD-202106-622 | |
| | | | CNNVD-202106-638 | |
| | | | CNNVD-202106-616 | |
| | | | CNNVD-202106-590 | |
| | | | CNNVD-202106-627 | |
| | | | CNNVD-202106-629 | |
| | | | CNNVD-202106-626 | |
| | | | CNNVD-202106-631 | |
| | | CNNVD-202106-610 | | |
| | | Siemens | CNNVD-202106-532 | |
| | | | CNNVD-202106-542 | |
| | | | CNNVD-202106-565 | |
| | | | CNNVD-202106-561 | |
| | | CNNVD-202106-539 | | |
| | | Softing | CNNVD-202106-1370 | |
| | | WIBU | CNNVD-202106-1303 | |
| | | patek | CNNVD-202106-1654 | |
| | | | CNNVD-202106-1655 | |
| | | | CNNVD-202106-1652 | |
| | | 个人开发者 | CNNVD-202106-772 | |
| | | | CNNVD-202106-077 | |

| | | | | |
|------------------|-------------------|------------------------|-------------------|--|
| | | | CNNVD-202106-777 | |
| | | | CNNVD-202106-773 | |
| | | | CNNVD-202106-1435 | |
| | | | CNNVD-202106-784 | |
| | | | CNNVD-202106-1424 | |
| | | | CNNVD-202106-1436 | |
| | | | CNNVD-202106-103 | |
| 6 | 访问控制 错误 | AVEVA | CNNVD-202106-1951 | IBM Engineering Systems Design Rhapsody 访问控制错误漏洞 (CNNVD-202106-030) |
| | | Bosch | CNNVD-202106-242 | |
| | | Gallagher | CNNVD-202106-963 | |
| | | Huawei | CNNVD-202106-244 | |
| | | | CNNVD-202106-234 | |
| | | IBM | CNNVD-202106-030 | |
| | | Intel | CNNVD-202106-690 | |
| | | Nextcloud | CNNVD-202106-110 | |
| | | QNAP Systems | CNNVD-202106-1194 | |
| | | Samsung | CNNVD-202106-953 | |
| | | TIBCO Software | CNNVD-202106-1948 | |
| | | | CNNVD-202106-1947 | |
| | | Western Digital | CNNVD-202106-1959 | |
| | | WordPress 基金会 | CNNVD-202106-1224 | |
| | | | CNNVD-202106-1220 | |
| | | | CNNVD-202106-1219 | |
| ZTE | CNNVD-202106-791 | | | |
| Zammad | CNNVD-202106-1914 | | | |
| 个人开发者 | CNNVD-202106-1594 | | | |
| 7 | 资源管理 错误 | Adobe | CNNVD-202106-484 | Microsoft Edge 资源管理错误漏洞 (CNNVD-202106-1377) |
| | | | CNNVD-202106-482 | |
| | | | CNNVD-202106-483 | |
| | | Apache 基金会 | CNNVD-202106-1306 | |
| | | Apple | CNNVD-202106-1240 | |
| | | Autodesk | CNNVD-202106-1599 | |
| | | | CNNVD-202106-1595 | |
| | | Google | CNNVD-202106-760 | |
| | | | CNNVD-202106-419 | |
| | | | CNNVD-202106-753 | |
| | | | CNNVD-202106-430 | |
| | | | CNNVD-202106-763 | |
| | | | CNNVD-202106-759 | |
| | | | CNNVD-202106-765 | |
| CNNVD-202106-398 | | | | |
| CNNVD-202106-755 | | | | |
| CNNVD-202106-428 | | | | |

| | | | | |
|-------------------------|-------------------|-----------------------------|-------------------|--|
| | | | CNNVD-202106-761 | |
| | | | CNNVD-202106-766 | |
| | | | CNNVD-202106-433 | |
| | | | CNNVD-202106-418 | |
| | | Gtlab | CNNVD-202106-264 | |
| | | Huawei | CNNVD-202106-770 | |
| | | Linux 基金会 | CNNVD-202106-399 | |
| | | | CNNVD-202106-416 | |
| | | | CNNVD-202106-414 | |
| | | | CNNVD-202106-410 | |
| | | MOXA | CNNVD-202106-1408 | |
| | | | CNNVD-202106-1407 | |
| | | Microsoft | CNNVD-202106-1377 | |
| | | | CNNVD-202106-1376 | |
| | | | CNNVD-202106-1378 | |
| | | | CNNVD-202106-1375 | |
| | | Mobatek | CNNVD-202106-220 | |
| | | Open Design Alliance | CNNVD-202106-688 | |
| | | Opentext | CNNVD-202106-194 | |
| | | | CNNVD-202106-155 | |
| | | Schneider Electric | CNNVD-202106-601 | |
| | | Siemens | CNNVD-202106-475 | |
| | | Ubiquiti Networks | CNNVD-202106-1410 | |
| | | | CNNVD-202106-1438 | |
| | | 个人开发者 | CNNVD-202106-1409 | |
| | | | CNNVD-202106-781 | |
| | | | CNNVD-202106-1615 | |
| | | | CNNVD-202106-778 | |
| 8 | 输入验证错误 | Arch | CNNVD-202106-089 | 微软 Visual Studio 输入验证错误漏洞 (CNNVD-202106-495) |
| | | FFmpeg | CNNVD-202106-240 | |
| | | Google | CNNVD-202106-386 | |
| | | HelpU | CNNVD-202106-1675 | |
| | | Huawei | CNNVD-202106-343 | |
| | | | CNNVD-202106-1883 | |
| | | IBM | CNNVD-202106-1721 | |
| | | Intel | CNNVD-202106-698 | |
| | | Microsoft | CNNVD-202106-506 | |
| | | | CNNVD-202106-495 | |
| | | | CNNVD-202106-490 | |
| NVIDIA | CNNVD-202106-1473 | | | |
| Pivotal Software | CNNVD-202106-093 | | | |

| | | | | |
|-------------------|--|---------------------------|-------------------|--|
| | | SAP | CNNVD-202106-456 | |
| | | | CNNVD-202106-469 | |
| | | | CNNVD-202106-460 | |
| | | | CNNVD-202106-455 | |
| | | | CNNVD-202106-458 | |
| | | | CNNVD-202106-471 | |
| | | | CNNVD-202106-476 | |
| | | | CNNVD-202106-457 | |
| | | | CNNVD-202106-472 | |
| | | Samsung | CNNVD-202106-958 | |
| | | Schneider Electric | CNNVD-202106-999 | |
| | | TP-Link | CNNVD-202106-805 | |
| | | Vmware | CNNVD-202106-1540 | |
| | | ZOHO | CNNVD-202106-788 | |
| | | 个人开发者 | CNNVD-202106-167 | |
| CNNVD-202106-1010 | | | | |
| CNNVD-202106-730 | | | | |
| CNNVD-202106-786 | | | | |

1. Microsoft Office SharePoint 代码问题漏洞 (CNNVD-202106-492)

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 Office SharePoint 存在安全漏洞。以下产品和版本受到影响：Microsoft SharePoint Enterprise Server 2016, Microsoft SharePoint Server 2019, Microsoft SharePoint Foundation 2013 Service Pack 1。

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/en-US/security-guidance/advisory/CVE-2021-31950>

2. Rockwell Automation Connected Components Workbench 代

码问题漏洞（CNNVD-202105-805）

Rockwell Automation Connected Components Workbench 是美国罗克韦尔（Rockwell Automation）公司的一个应用软件。一个自动编程软件。

Connected Components Workbench 12.00.00 版本及之前存在代码问题漏洞。该漏洞源于程序的组件工作台不限制可以反序列化的对象，攻击者可以利用该漏洞远程执行代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1131435

3. Intel Virtualization 授权问题漏洞（CNNVD-202106-630）

Intel Virtualization Technology for Direct I/O（Intel VT-d）是美国英特尔（Intel）公司的 Intel 虚拟化技术的一部分，主要针对的是 I/O 子系统，它的实现主要是通过通过在硬件上引入重定向单元，该硬件重定向单元用于对 I/O 子系统的 DMA 操作和中断传递进行重定向，从而辅助 VMM（Virtual Machine Monitor）实现 I/O 子系统的虚拟化。

Intel Virtualization Technology for Direct I/O（Intel VT-d）存在授权问题漏洞，该漏洞源于网络系统或产品中缺少身份验证措施或身份验证强度不足。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

<https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00442.html>

4. Fortinet FortiWeb 操作系统命令注入漏洞 (CNNVD-202106-013)

Fortinet FortiWeb 是美国飞塔 (Fortinet) 公司的一款 Web 应用层防火墙, 它能够阻断如跨站点脚本、SQL 注入、Cookie 中毒、schema 中毒等攻击的威胁, 保证 Web 应用程序的安全性并保护敏感的数据库内容。

Fortinet FortiWeb 存在操作系统命令注入漏洞, 该漏洞源于 FortiWeb 管理界面中的操作系统命令注入漏洞可能允许远程认证攻击者通过 SAML 服务器配置页面在系统上执行任意命令。以下产品和版本受到影响: FortiWeb: 6.3.7 版本及之前版本, 6.2.3 版本及之前版本, 6.1.x, 6.0.x, 5.9.x。

目前厂商已发布升级补丁以修复漏洞, 补丁获取链接:

<https://www.fortiguard.com/psirt/FG-IR-20-120>

5. Adobe After Effects 缓冲区错误漏洞 (CNNVD-202106-646)

Adobe After Effects 是美国奥多比 (Adobe) 公司的一套视觉效果和动态图形制作软件。该软件主要用于 2D 和 3D 合成、动画制作和视觉特效制作等。

Adobe After Effects 存在缓冲区错误漏洞, 该漏洞源于程序处理不可信输入时出现边界错误, 远程攻击者利用该漏洞可以创建一个专门制作的文件, 诱骗受害者使用受影响的软件打开它, 在目标系统上触发越界写入和执行任意代码。以下产品和版本受到影响: Adobe After Effects 10.0, 10.0.1, 10.0.2, 10.5, 10.5.1, 11.0, 11.0.1, 11.0.2, 12.0,

12.1, 12.2, 13.0, 13.1, 13.2, 13.5.0.347, 13.6.0, 13.7.0, 13.8.0, 14.0, 14.1, 14.2, 14.2.1, 15.0, 15.0.1, 15.1, 15.1.1, 15.1.2, 16.0, 16.0.1, 16.1, 16.1.2, 17.0.0, 17.0.1, 17.0.3, 17.0.6, 17.1, 17.1.1, 17.1.3, 18.0, 18.1, 18.2。

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/after_effects/apsb21-49.html

6. IBM Engineering Systems Design Rhapsody 访问控制错误漏洞（CNNVD-202106-030）

IBM Engineering Systems Design Rhapsody 是美国 IBM 公司的 IBM Engineering 产品组合的一部分。它为支持 UML、SysML、UAF 和 AUTOSAR 的系统工程师提供协作设计开发和测试环境。

IBM Engineering 存在访问控制错误漏洞，该漏洞源于 IBM Engineering Systems Design Rhapsody - Model Manager 未正确限制来自未授权角色的资源访问。攻击者可利用该漏洞绕过不正确的访问控制造成的安全限制。通过向 REST API 发送专门设计的请求，绕过访问限制，并使用管理权限执行任意操作。

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/6457739>

7. Microsoft Edge 资源管理错误漏洞（CNNVD-202106-1377）

Microsoft Edge 是美国微软（Microsoft）公司的一款 Windows 10 之后版本系统附带的 Web 浏览器。

Microsoft Edge (Chromium-based)存在资源管理错误漏洞。目前尚

无此漏洞的相关信息，请随时关注 CNNVD 或厂商公告。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-30555>

8. 微软 Visual Studio 输入验证错误漏洞(CNNVD-202106-495)

Microsoft Visual Studio 是美国微软（Microsoft）公司的一款开发工具套件系列产品，也是一个基本完整的开发工具集，它包括了整个软件生命周期所需要的大部分工具。

.NET Core & Visual Studio 存在安全漏洞。以下产品和版本受到影响：Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3), Microsoft Visual Studio 2019 version 16.7 (includes 16.0 - 16.6), Microsoft Visual Studio 2019 version 16.9 (includes 16.0 - 16.8), Microsoft Visual Studio 2019 version 16.10 (includes 16.0 - 16.9), Visual Studio 2019 for Mac version 8.10, .NET Core 3.1, .NET 5.0。

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/en-US/security-guidance/advisory/CVE-2021-31957>

二、漏洞平台推送情况

本周漏洞平台推送漏洞 5857 个。

表 7 2021 年 6 月漏洞平台推送情况

| 序号 | 漏洞平台 | 漏洞总量 |
|----|------|------|
|----|------|------|

| | | |
|------|------|------|
| 1 | 漏洞盒子 | 3965 |
| 2 | 补天平台 | 1892 |
| 推送总计 | | 5857 |

三、接报漏洞情况

本月接报漏洞 2214 个，其中信息技术产品漏洞（通用型漏洞）256 个，网络信息系统漏洞（事件型漏洞）1958 个。

表 8 2021 年 6 月漏洞接报情况

| 序号 | 报送单位 | 漏洞总量 |
|----|------------------|------|
| 1 | 河南听潮盛世信息技术有限公司 | 559 |
| 2 | 北京山石网科信息技术有限公司 | 358 |
| 3 | 奥创科技 | 227 |
| 4 | 微步在线科技有限公司 | 165 |
| 5 | 山东新潮信息技术有限公司 | 94 |
| 6 | 南京众智维信息科技有限公司 | 85 |
| 7 | 北京启明星辰信息安全技术有限公司 | 77 |
| 8 | 太极计算机股份有限公司 | 73 |
| 9 | 北京天地和兴科技有限公司 | 65 |
| 10 | 北京数字观星科技有限公司 | 50 |
| 11 | 中兴通讯 | 36 |
| 12 | 广州竞远安全技术股份有限公司 | 36 |
| 13 | 北京安帝科技有限公司 | 33 |
| 14 | 长春嘉诚信息技术股份有限公司 | 32 |
| 15 | 北京优炫软件股份有限公司 | 27 |

| | | |
|----|------------------------|----|
| 16 | 浙江大华技术股份有限公司 | 25 |
| 17 | 西安四叶草信息技术有限公司 | 23 |
| 18 | 北京鸿腾智能科技有限公司 | 20 |
| 19 | 远江盛邦（北京）网络安全科技股份有限公司 | 20 |
| 20 | 绿盟科技集团股份有限公司 | 17 |
| 21 | 个人 | 16 |
| 22 | 北京华胜久安科技有限公司 | 15 |
| 23 | 安徽长泰信息安全服务有限公司 | 15 |
| 24 | 山东云天安全技术有限公司 | 15 |
| 25 | 上海上讯信息技术股份有限公司 | 12 |
| 26 | 恒安嘉新（北京）科技股份公司 | 12 |
| 27 | 清华大学网络科学与网络空间研究院 | 9 |
| 28 | 上海安几科技有限公司 | 8 |
| 29 | 北京云测信息技术有限公司 | 7 |
| 30 | 杭州安恒信息技术股份有限公司 | 7 |
| 31 | 江苏通付盾科技有限公司 | 7 |
| 32 | 北京天融信网络安全技术有限公司 | 6 |
| 33 | 北京安帝科技有限公司 andisec 实验室 | 6 |
| 34 | 南京赛宁信息技术有限公司 | 6 |
| 35 | 重庆梦之想科技有限责任公司 | 6 |
| 36 | 内蒙古思沃科技有限公司 | 5 |
| 37 | 网神信息技术（北京）股份有限公司 | 5 |
| 38 | 北京容辉智信科技有限公司 | 4 |

| | | |
|------|------------------|------|
| 39 | 杭州海康威视数字技术股份有限公司 | 4 |
| 40 | 上海市安几科技有限公司 | 3 |
| 41 | 内蒙古中叶信息技术有限责任公司 | 3 |
| 42 | 华为技术有限公司 | 3 |
| 43 | 杭州华为企业通信技术有限公司 | 3 |
| 44 | 北京威努特技术有限公司 | 2 |
| 45 | 北京首华建设经营有限公司 | 2 |
| 46 | 华胜久安 | 2 |
| 47 | 北京信联科汇科技有限公司 | 1 |
| 48 | 北京国舜科技股份有限公司 | 1 |
| 49 | 北京时代新威信息技术有限公司 | 1 |
| 50 | 四川创腾科技有限公司 | 1 |
| 51 | 安全邦（北京）信息技术有限公司 | 1 |
| 52 | 山东正中信息技术股份有限公司 | 1 |
| 53 | 山东泽鹿安全技术有限公司 | 1 |
| 54 | 湖南中测网安信息技术有限公司 | 1 |
| 55 | 默安科技有限公司 | 1 |
| 报送总计 | | 2214 |

四、重大漏洞预警

4.1 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 Windows Defender 安全漏洞(CNNVD-202106-545、CVE-2021-31985)、Microsoft

Office Excel 安全漏洞（CNNVD-202106-503、CVE-2021-31939）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

2021年6月9日，微软发布了2021年6月份安全更新，共49个漏洞的补丁程序，CNNVD对这些漏洞进行了收录。本次更新主要涵盖了Windows操作系统、Net Core、Office、Edge、SharePoint Server、Hyper-V、Visual Studio等。CNNVD对其危害等级进行了评价，其中高危漏洞有15个，中危漏洞34个。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。

. 漏洞详情

此次更新共包括49个漏洞的补丁程序，其中高危漏洞有15个，中危漏洞34个。

| 序号 | 漏洞名称 | CNNVD 编号 | CVE 编号 | 危害等级 | 官方链接 |
|----|-----------------------------|------------------|----------------|------|---|
| 1 | Microsoft Office Excel 安全漏洞 | CNNVD-202106-503 | CVE-2021-31939 | 高危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31939 |
| 2 | Microsoft Office 安全漏洞 | CNNVD-202106-504 | CVE-2021-31940 | 高危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31940 |
| 3 | Microsoft Office 安全漏洞 | CNNVD-202106-500 | CVE-2021-31941 | 高危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31941 |

| | | | | | |
|----|---------------------------------------|------------------|----------------|----|---|
| 4 | 3D Viewer 安全漏洞 | CNNVD-202106-518 | CVE-2021-31942 | 高危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31942 |
| 5 | 3D Viewer 安全漏洞 | CNNVD-202106-517 | CVE-2021-31943 | 高危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31943 |
| 6 | Paint 3D 安全漏洞 | CNNVD-202106-522 | CVE-2021-31945 | 高危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31945 |
| 7 | Paint 3D 安全漏洞 | CNNVD-202106-525 | CVE-2021-31946 | 高危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31946 |
| 8 | Windows NTFS 安全漏洞 | CNNVD-202106-515 | CVE-2021-31956 | 高危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31956 |
| 9 | Windows Kerberos 安全漏洞 | CNNVD-202106-534 | CVE-2021-31962 | 高危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31962 |
| 10 | Microsoft Windows Codecs Library 安全漏洞 | CNNVD-202106-537 | CVE-2021-31967 | 高危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31967 |
| 11 | Microsoft Intune 安全漏洞 | CNNVD-202106-535 | CVE-2021-31980 | 高危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31980 |
| 12 | Paint 3D 安全漏洞 | CNNVD-202106-524 | CVE-2021-31983 | 高危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31983 |
| 13 | Windows Defender 安全漏洞 | CNNVD-202106-545 | CVE-2021-31985 | 高危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31985 |
| 14 | Microsoft DWM Core Library 安全漏洞 | CNNVD-202106-498 | CVE-2021-33739 | 高危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33739 |
| 15 | Windows MSHTML Platform 安全漏洞 | CNNVD-202106-497 | CVE-2021-33742 | 高危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33742 |
| 16 | Windows Print Spooler Components 安 | CNNVD-202106-513 | CVE-2021-1675 | 中危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1675 |

| | | | | | |
|----|---|----------------------|--------------------|----|---|
| | 全漏洞 | | | | |
| 17 | Windows DCOM Server 安全漏洞 | CNNVD-20 2106-546 | CVE-2021 -26414 | 中危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26414 |
| 18 | Microsoft Office SharePoint 安全 漏洞 | CNNVD-20 2106-491 | CVE-2021 -26420 | 中危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26420 |
| 19 | Windows Cryptographic Services 安全漏 洞 | CNNVD-20 2106-540 | CVE-2021 -31199 | 中危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31199 |
| 20 | Windows Cryptographic Services 安全漏 洞 | CNNVD-20 2106-541 | CVE-2021 -31201 | 中危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31201 |
| 21 | Visual Studio Code 安全漏洞 | CNNVD-20 2106-538 | CVE-2021 -31938 | 中危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31938 |
| 22 | 3D Viewer 安全 漏洞 | CNNVD-20 2106-521 | CVE-2021 -31944 | 中危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31944 |
| 23 | Microsoft Office SharePoint 安全 漏洞 | CNNVD-20 2106-490 | CVE-2021 -31948 | 中危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31948 |
| 24 | Microsoft Office Outlook 安全漏 洞 | CNNVD-20 2106-499 | CVE-2021 -31949 | 中危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31949 |
| 25 | Microsoft Office SharePoint 安全 漏洞 | CNNVD-20 2106-492 | CVE-2021 -31950 | 中危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31950 |
| 26 | Windows Kernel 安全漏洞 | CNNVD-20 2106-543 | CVE-2021 -31951 | 中危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31951 |
| 27 | Windows Kernel-Mode Drivers 安全漏 洞 | CNNVD-20 2106-514 | CVE-2021 -31952 | 中危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31952 |

| | | | | | |
|----|--|------------------|----------------|----|---|
| 28 | Microsoft Windows和 Vulnerability 权限许可和访问控制问题漏洞 | CNNVD-202106-509 | CVE-2021-31953 | 中危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31953 |
| 29 | Windows Common Log File System Driver 安全漏洞 | CNNVD-202106-508 | CVE-2021-31954 | 中危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31954 |
| 30 | Windows Kernel 安全漏洞 | CNNVD-202106-516 | CVE-2021-31955 | 中危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31955 |
| 31 | Visual Studio 安全漏洞 | CNNVD-202106-495 | CVE-2021-31957 | 中危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31957 |
| 32 | Windows NTLM 安全漏洞 | CNNVD-202106-512 | CVE-2021-31958 | 中危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31958 |
| 33 | Microsoft Scripting Engine 安全漏洞 | CNNVD-202106-505 | CVE-2021-31959 | 中危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31959 |
| 34 | Windows Bind Filter Driver 安全漏洞 | CNNVD-202106-536 | CVE-2021-31960 | 中危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31960 |
| 35 | Microsoft Office SharePoint 安全漏洞 | CNNVD-202106-496 | CVE-2021-31963 | 中危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31963 |
| 36 | Microsoft Office SharePoint 安全漏洞 | CNNVD-202106-487 | CVE-2021-31964 | 中危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31964 |
| 37 | Microsoft Office SharePoint 安全漏洞 | CNNVD-202106-488 | CVE-2021-31965 | 中危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31965 |
| 38 | Microsoft Office SharePoint 安全漏洞 | CNNVD-202106-489 | CVE-2021-31966 | 中危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31966 |
| 39 | Windows Remote Desktop 安全漏洞 | CNNVD-202106-531 | CVE-2021-31968 | 中危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31968 |

| | | | | | |
|----|------------------------------------|------------------|----------------|----|---|
| 40 | Windows Drivers 安全漏洞 | CNNVD-202106-527 | CVE-2021-31969 | 中危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31969 |
| 41 | Windows TCP/IP 安全漏洞 | CNNVD-202106-520 | CVE-2021-31970 | 中危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31970 |
| 42 | Windows HTML Platform 安全漏洞 | CNNVD-202106-519 | CVE-2021-31971 | 中危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31971 |
| 43 | Windows Event Logging Service 安全漏洞 | CNNVD-202106-511 | CVE-2021-31972 | 中危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31972 |
| 44 | Windows Installer 安全漏洞 | CNNVD-202106-510 | CVE-2021-31973 | 中危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31973 |
| 45 | Windows Network File System 安全漏洞 | CNNVD-202106-506 | CVE-2021-31974 | 中危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31974 |
| 46 | Windows Network File System 安全漏洞 | CNNVD-202106-507 | CVE-2021-31975 | 中危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31975 |
| 47 | Windows Network File System 安全漏洞 | CNNVD-202106-502 | CVE-2021-31976 | 中危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31976 |
| 48 | Hyper-V 安全漏洞 | CNNVD-202106-501 | CVE-2021-31977 | 中危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31977 |
| 49 | Windows Defender 安全漏洞 | CNNVD-202106-544 | CVE-2021-31978 | 中危 | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31978 |

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。微软官方补丁下载地址：

<https://msrc.microsoft.com/update-guide/en-us>

4.2 用友 NC BeanShell 远程代码执行漏洞的预警

近日，国家信息安全漏洞库（CNNVD）收到关于用友 NC BeanShell 远程代码执行漏洞（CNNVD-202106-205）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。用友 NC 6.5 版本受此漏洞影响。目前，用友官方已经发布了解决方案修复了漏洞，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

用友 NC 是中国用友集团旗下一款面向集团企业的管理软件。用友 NC 存在远程代码执行漏洞，该漏洞源于用友 NC 对外开放了 BeanShell 接口，攻击者可以在未授权的情况下直接访问该接口，并构造恶意数据执行任意代码，从而获取服务器权限。

. 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。用友 NC 6.5 版本受此漏洞影响。

. 修复建议

目前，用友官方已经发布了解决方案修复了漏洞，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。授权用户可以访问下载链接进行下载：

<http://umc.yonyou.com/ump/querypatchdetailedmng?PK=18981c7af483007db179a236016f594d37c01f22aa5f5d19>