# 信息安全漏洞通报

**2020 年 12 月** **国家信息安全漏洞库（CNNVD）**

## 本 期 导 读

### 漏洞态势

根据国家信息安全漏洞库（CNNVD）统计，2020 年 12 月份采集安全漏洞共 1535 个。

本月接报漏洞 58601 个，其中信息技术产品漏洞（通用型漏洞）192 个，网络信息系统漏洞（事件型漏洞）58409 个。

### 重大漏洞预警

Apache Struts2 S2-061 远程代码执行漏洞（CNNVD-202012-449、CVE-2020-17530）：成功利用漏洞的攻击者可以在目标系统执行恶意代码。Apache Struts 2.0.0 - 2.5.25 版本均受此漏洞影响。目前，Apache 官方已经发布了版本更新修复了该漏洞。建议用户及时确认产品版本，尽快采取修补措施。

微软多个安全漏洞：包括 Microsoft Exchange Server 安全漏洞（CNNVD-202012-615、CVE-2020-17117）、Microsoft SharePoint 安全漏洞（CNNVD-202012-620、CVE-2020-17118）等多个安全漏洞，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 12 月份新增安全漏洞共 1535 个，从厂商分布来看，Google 公司产品的漏洞数量最多，共发布 146 个；从漏洞类型来看，跨站脚本类的漏洞占比最大，达到 12.25%。本月新增漏洞中，超危漏洞 251 个、高危漏洞 499 个、中危漏洞 737 个、低危漏洞 48 个，相应修复率分别为 68.53%、88.78%、83.72%以及 95.83%。合计 1278 个漏洞已有修复补丁发布，本月整体修复率 83.26%。

截至 2020 年 12 月 31 日，CNNVD 采集漏洞总量已达 155724 个。

### 1.1 漏洞增长概况

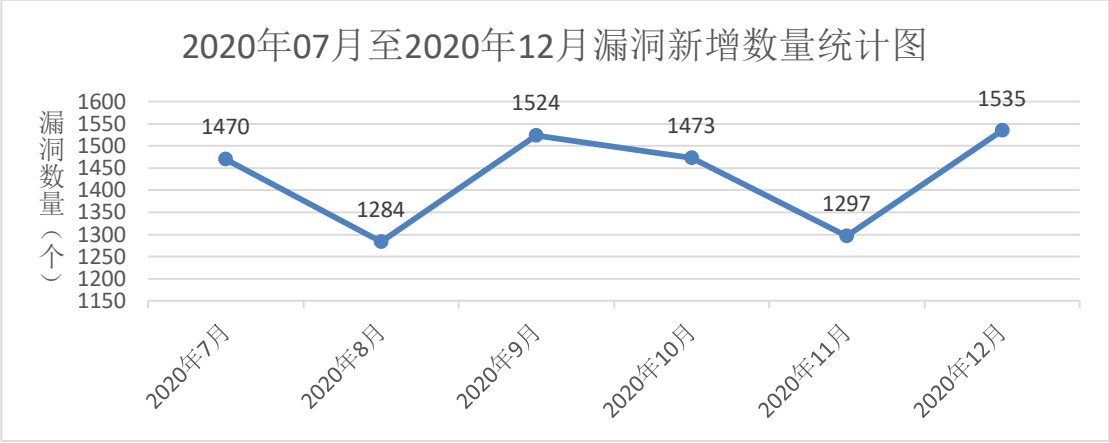


图 1 2020 年 7 月至 2020 年 12 月漏洞新增数量统计图

2020 年 12 月新增安全漏洞 1535 个，与上月（1297 个）相比增加了 18.35%。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 1431 个。

## 1.2 漏洞分布情况

### 1.2.1 漏洞厂商分布

12 月厂商漏洞数量分布情况如表 1 所示，Google 公司漏洞达到 146 个，占本月漏洞总量的 9.51%。

表 1　2020 年 12 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** | Google | 146 | 9.51% |
| **2** | Mozilla 基金会 | 98 | 6.38% |
| **3** | NETGEAR | 66 | 4.30% |
| **4** | Microsoft | 62 | 4.04% |
| **5** | Apple | 47 | 3.06% |
| **6** | Docker | 35 | 2.28% |
| **7** | ImageMagick Studio | 34 | 2.21% |
| **8** | WordPress 基金会 | 28 | 1.82% |
| **9** | IBM | 27 | 1.76% |
| **10** | F5 | 21 | 1.37% |

### 1.2.2 漏洞产品分布

12 月主流操作系统的漏洞统计情况如表 2 所示。本月 Android 漏洞数量最多，共 119 个，占主流操作系统漏洞总量的 58.33%，排名第一。

表 2　2020 年 12 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** | Android | 119 |
| **2** | Windows 10 | 20 |

| | | |
|---|---|---|
| **3** | Windows Server 2019 | 12 |
| **4** | Windows Server 2016 | 10 |
| **5** | Windows 7 | 9 |
| **6** | Windows Server 2012 | 6 |
| **7** | Windows Server 2012 R2 | 6 |
| **8** | Linux Kernel | 6 |
| **9** | Windows 8.1 | 5 |
| **10** | Windows Rt 8.1 | 5 |
| **11** | Windows Server 2008 | 3 |
| **12** | Windows Server 2008 R2 | 3 |

### 1.2.3 漏洞类型分布

12 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 12.25%。

表 3 2020 年 12 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 | 188 | 12.25% |
| 2 | 缓冲区错误 | 144 | 9.38% |
| 3 | 输入验证错误 | 107 | 6.97% |
| 4 | 代码问题 | 90 | 5.86% |
| 5 | 授权问题 | 71 | 4.63% |
| 6 | 信息泄露 | 65 | 4.23% |
| 7 | 资源管理错误 | 56 | 3.65% |
| 8 | 访问控制错误 | 56 | 3.65% |
| 9 | SQL 注入 | 52 | 3.39% |
| 10 | 跨站请求伪造 | 29 | 1.89% |
| 11 | 命令注入 | 26 | 1.69% |
| 12 | 路径遍历 | 24 | 1.56% |
| 13 | 操作系统命令注入 | 20 | 1.30% |
| 14 | 信任管理问题 | 18 | 1.17% |
| 15 | 权限许可和访问控制问题 | 18 | 1.17% |
| 16 | 代码注入 | 16 | 1.04% |
| 17 | 注入 | 13 | 0.85% |
| 18 | 加密问题 | 10 | 0.65% |
| 19 | 数字错误 | 5 | 0.33% |
| 20 | 数据伪造问题 | 4 | 0.26% |
| 21 | 后置链接 | 4 | 0.26% |
| 22 | 默认配置问题 | 3 | 0.20% |

| | | | |
|---|---|---|---|
| 23 | 日志信息泄露 | 2 | 0.13% |
| 24 | 安全特征问题 | 2 | 0.13% |
| 25 | 处理逻辑错误 | 2 | 0.13% |
| 26 | 竞争条件问题 | 1 | 0.07% |
| 27 | 环境问题 | 1 | 0.07% |
| 28 | 参数注入 | 1 | 0.07% |
| 29 | 其他 | 462 | 30.10% |

### 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。12 月漏洞危害等级分布如图 2 所示，其中超危漏洞 251 条，占本月漏洞总数的 16.35%。

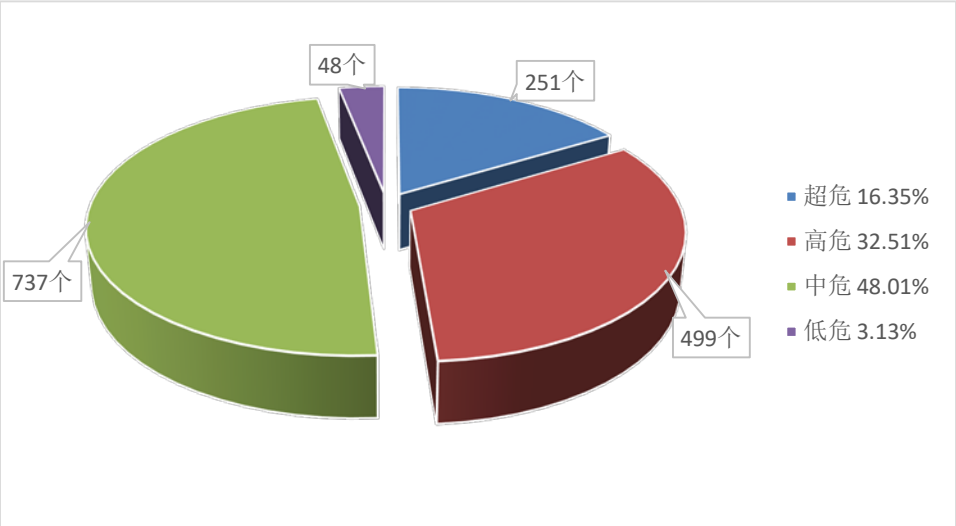


图 2　2020 年 12 月漏洞危害等级分布

## 1.3 漏洞修复情况

### 1.3.1　整体修复情况

12 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 95.83%，超危漏洞修复率最低，比例为 68.53%。总体来看，本月整体修复率，由上月的 89.67%下降至本月的 83.26%。

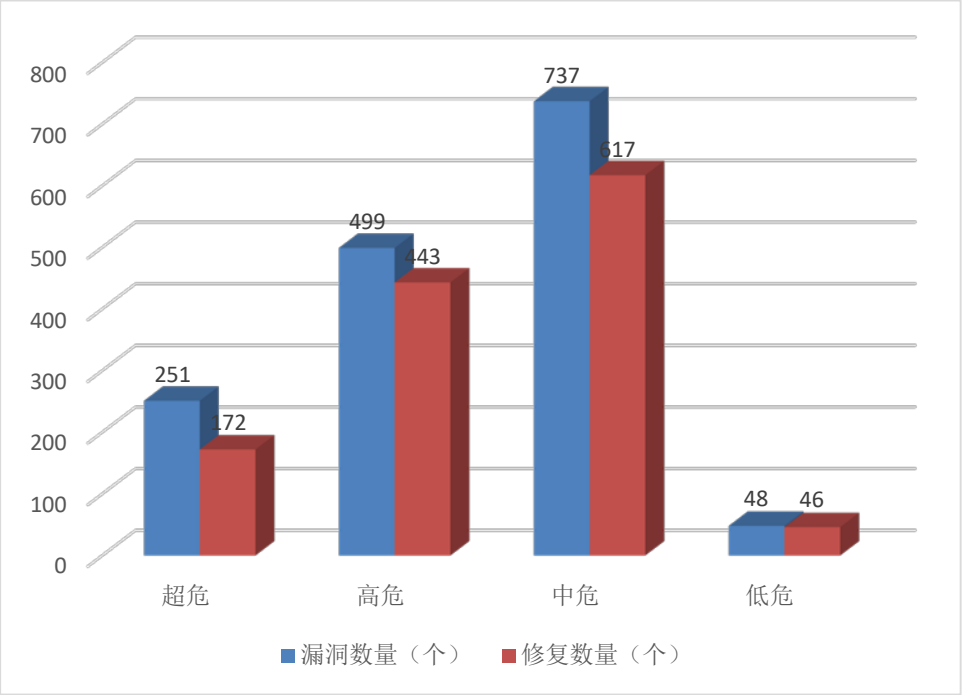


图 3　2020 年 12 月漏洞修复数量统计

### 1.3.2　厂商修复情况

12 月漏洞修复情况按漏洞数量前十厂商进行统计，其中 Google、Mozilla 基金会、NETGEAR 等十个厂商共 564 条漏洞，占本月漏洞总数的 36.74%，漏洞修复率为 91.13%，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 NETGEAR、Apple、WordPress 基金会、IBM、F5 等公司本月漏洞修复率均为 100%，共 514 条漏洞已全部修复。

表 4　2020 年 12 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 | Google | 146 | 142 | 97.26% |
| 2 | Mozilla 基金会 | 98 | 78 | 79.59% |
| 3 | NETGEAR | 66 | 66 | 100.00% |
| 4 | Microsoft | 62 | 60 | 96.77% |
| 5 | Apple | 47 | 47 | 100.00% |
| 6 | Docker | 35 | 12 | 34.29% |
| 7 | ImageMagick Studio | 34 | 33 | 97.06% |
| 8 | WordPress 基金会 | 28 | 28 | 100.00% |

| | | | | |
|---|---|---|---|---|
| 9 | IBM | 27 | 27 | 100.00% |
| 10 | F5 | 21 | 21 | 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 251 个，其中重要漏洞实例如表 5 所示。

表 5　2020 年 12 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-202012-1468 | ABB | Sophos Cyberoam OS SQL 注入漏洞（CNNVD-202012-982） |
| | | CNNVD-202012-1703 | Agentejo | |
| | | CNNVD-202012-1706 | | |
| | | CNNVD-202012-1704 | | |
| | | CNNVD-202012-1359 | Bilanc Shpk | |
| | | CNNVD-202012-1555 | Egavilan Media | |
| | | CNNVD-202012-1553 | | |
| | | CNNVD-202012-1455 | Egavilanmedia | |
| | | CNNVD-202012-1512 | Grupo Crk | |
| | | CNNVD-202012-1616 | Open Source Matters | |
| | | CNNVD-202012-041 | PHP Scripts Mall | |
| | | CNNVD-202012-043 | PHPGroup | |
| | | CNNVD-202012-951 | PHPSHE | |
| | | CNNVD-202012-982 | Sophos | |
| | | CNNVD-202012-036 | SourceCodester | |
| | | CNNVD-202012-1021 | Sourcecodester | |
| | | CNNVD-202012-1263 | | |
| | | CNNVD-202012-1251 | | |
| | | CNNVD-202012-037 | | |
| | | CNNVD-202012-1277 | | |
| | | CNNVD-202012-1264 | Spotweb 团队 | |
| | | CNNVD-202012-042 | USSourceCodester | |
| | | CNNVD-202012-1360 | Weiphp | |
| | | CNNVD-202012-007 | ZXELINK | |
| | | CNNVD-202012-058 | 个人开发者 | |

| | | | | |
|---|---|---|---|---|
| | | CNNVD-202012-1589 | | |
| | | CNNVD-202012-1004 | | |
| | | CNNVD-202012-1431 | | |
| | | CNNVD-202012-1590 | | |
| | | CNNVD-202012-1430 | | |
| | | CNNVD-202012-1586 | | |
| | | CNNVD-202012-685 | | |
| | | CNNVD-202012-1585 | | |
| | | CNNVD-202012-035 | | |
| **2** | 代码问题 | CNNVD-202012-686 | Apache 基金会 | Apache Tapestry 代码问题漏洞（CNNVD-202012-686） |
| | | CNNVD-202012-1566 | Esri | |
| | | CNNVD-202012-1429 | Kronos | |
| | | CNNVD-202012-1236 | Kyland | |
| | | CNNVD-202012-841 | LAN ATMservice | |
| | | CNNVD-202012-1014 | Quantconnect | |
| | | CNNVD-202012-1502 | Terramaster | |
| | | CNNVD-202012-1289 | Wordpress 基金会 | |
| | | CNNVD-202012-1271 | 个人开发者 | |
| | | CNNVD-202012-678 | | |
| | | CNNVD-202012-431 | | |
| **3** | 授权问题 | CNNVD-202012-1467 | ABB | SAP Netweaver 授权问题漏洞（CNNVD-202012-575） |
| | | CNNVD-202012-1192 | AdRem | |
| | | CNNVD-202012-1257 | Apache 基金会 | |
| | | CNNVD-202012-855 | Cisco | |
| | | CNNVD-202012-957 | Docker | |
| | | CNNVD-202012-961 | | |
| | | CNNVD-202012-975 | | |
| | | CNNVD-202012-1181 | EPSON | |
| | | CNNVD-202012-026 | HP | |
| | | CNNVD-202012-1032 | IBM | |
| | | CNNVD-202012-575 | SAP | |
| | | CNNVD-202012-1383 | Samsung | |
| | | CNNVD-202012-1595 | Solarwinds | |
| | | CNNVD-202012-1209 | Trend Micro | |
| | | CNNVD-202012-942 | Western Digital | |
| | | CNNVD-202012-1650 | Zammad | |
| | | CNNVD-202012-430 | 个人开发者 | |
| | | CNNVD-202012-1269 | | |

| | | | | |
|---|---|---|---|---|
| **4** | 操作系统命令注入 | CNNVD-202012-1569 | Belkin | Belkin LINKSYS RE6500 操作系统命令注入漏洞（CNNVD-202012-1569） |
| | | CNNVD-202012-567 | SAP | |
| | | CNNVD-202012-1548 | Terramaster | |
| | | CNNVD-202012-1513 | Urve | |
| | | CNNVD-202012-1303 | WAGO | |
| | | CNNVD-202012-1603 | 个人开发者 | |
| | | CNNVD-202012-836 | | |
| | | CNNVD-202012-834 | | |
| **5** | 缓冲区错误 | CNNVD-202012-788 | Apache 基金会 | Google Android 缓冲区错误漏洞（CNNVD-202012-556） |
| | | CNNVD-202012-787 | | |
| | | CNNVD-202012-014 | Edimax Technology | |
| | | CNNVD-202012-057 | Eipstackgroup | |
| | | CNNVD-202012-777 | Flexense | |
| | | CNNVD-202012-556 | Google | |
| | | CNNVD-202012-557 | | |
| | | CNNVD-202012-558 | | |
| | | CNNVD-202012-1027 | HCL | |
| | | CNNVD-202012-1353 | | |
| | | CNNVD-202012-1028 | IBM | |
| | | CNNVD-202012-782 | Jerryscript 项目 | |
| | | CNNVD-202012-1584 | Jiransecurity | |
| | | CNNVD-202012-858 | Medtronic | |
| | | CNNVD-202012-396 | Moddable | |
| | | CNNVD-202012-1347 | Treck | |
| | | CNNVD-202012-028 | Valvesoftware | |
| | | CNNVD-202012-089 | | |
| | | CNNVD-202012-653 | 个人开发者 | |
| | | CNNVD-202012-633 | | |
| | | CNNVD-202012-1025 | | |
| | | CNNVD-202012-636 | | |
| | | CNNVD-202012-641 | | |
| | | CNNVD-202012-629 | | |
| | | CNNVD-202012-644 | | |
| | | CNNVD-202012-663 | | |
| | | CNNVD-202012-634 | | |
| | | CNNVD-202012-638 | | |
| | | CNNVD-202012-630 | | |
| | | CNNVD-202012-635 | | |
| | | CNNVD-202012-659 | | |
| | | CNNVD-202012-070 | | |
| | | CNNVD-202012-1367 | | |

| | | | | |
|---|---|---|---|---|
| | | CNNVD-202012-1588 | | |
| | | CNNVD-202012-631 | | |
| | | CNNVD-202012-1026 | | |
| **6** | 访问控制错误 | CNNVD-202012-1496 | ABB | Siemens LOGO! 8 BM 访问控制错误漏洞（CNNVD-202012-695） |
| | | CNNVD-202012-1093 | Docker | |
| | | CNNVD-202012-047 | | |
| | | CNNVD-202012-1247 | | |
| | | CNNVD-202012-1094 | | |
| | | CNNVD-202012-1249 | | |
| | | CNNVD-202012-1088 | | |
| | | CNNVD-202012-1248 | | |
| | | CNNVD-202012-1250 | | |
| | | CNNVD-202012-1087 | | |
| | | CNNVD-202012-1086 | | |
| | | CNNVD-202012-1176 | | |
| | | CNNVD-202012-1246 | | |
| | | CNNVD-202012-1174 | | |
| | | CNNVD-202012-1239 | | |
| | | CNNVD-202012-1245 | | |
| | | CNNVD-202012-1244 | | |
| | | CNNVD-202012-1243 | | |
| | | CNNVD-202012-1238 | | |
| | | CNNVD-202012-1092 | | |
| | | CNNVD-202012-1091 | | |
| | | CNNVD-202012-1101 | | |
| | | CNNVD-202012-1241 | | |
| | | CNNVD-202012-1090 | | |
| | | CNNVD-202012-938 | Schneider Electric | |
| | | CNNVD-202012-695 | Siemens | |
| **7** | 信任管理问题 | CNNVD-202012-013 | Schneider Electric | Adrem Netcrunch 信任管理问题漏洞（CNNVD-202012-1191） |
| | | CNNVD-202012-1097 | Icinga | |
| | | CNNVD-202012-1191 | AdRem | |
| | | CNNVD-202012-1389 | Bilanc Shpk | |
| | | CNNVD-202012-1404 | Bilanc Shpk | |
| **8** | 输入验证错误 | CNNVD-202012-1463 | ABB | Cisco Jabber 输入验证错误漏洞（CNNVD-202012-852） |
| | | CNNVD-202012-857 | Cisco | |
| | | CNNVD-202012-852 | | |
| | | CNNVD-202012-031 | HCL | |
| | | CNNVD-202012-1481 | Odoo | |
| | | CNNVD-202012-1029 | Sourcecodester | |

| | | | | |
|---|---|---|---|---|
| | | CNNVD-202012-1208 | Sprymedia | |
| | | CNNVD-202012-1774 | Webmin 社区 | |
| | | CNNVD-202012-009 | Western Digital | |
| | | CNNVD-202012-1007 | 个人开发者 | |

**1. Sophos Cyberoam OS SQL 注入漏洞（CNNVD-202012-982）**

Sophos Cyberoam OS 是美国 Sophos 公司的一款用于 Cyberoam 设备的操作系统。

Sophos Cyberoam OS 2020-12-04 版本存在 SQL 注入漏洞，该漏洞源于 WebAdmin 中有一个 SQL 注入，允许未经身份验证的攻击者利用该漏洞远程执行任意 SQL 语句。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://support.sophos.com/support/s/article/KB-000040678?language=en_US

**2. Apache Tapestry 代码问题漏洞（CNNVD-202012-686）**

Apache Tapestry 是美国阿帕奇（Apache）基金会的一款使用 Java 语言编写的 Web 应用程序框架。

Apache Tapestry 4 存在安全漏洞，该漏洞源于在调用页面的验证方法之前尝试反序列化“sp”参数，这将导致在没有身份验证的情况下反序列化。

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/r700a6aa234dbff0555d4187bdc8274d7e4c0afbf35b9a3457f09ee76@%3Cusers.tapestry.apache.org%3E

**3. SAP Netweaver 授权问题漏洞（CNNVD-202012-575）**

SAP Netweaver 是德国思爱普（SAP）公司的一套面向服务的集成化应用平台。该平台主要为 SAP 应用程序提供开发和运行环境。

SAP NetWeaver 存在安全漏洞，该漏洞源于缺少身份验证检查，允许在集群之外，甚至在专门用于内部集群通信的网络权限之外的进程进行任意连接。以下产品及版本受到影：7.11,7.20,7.30,7.31,7.40,7.50。

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=564757079

4. **Belkin LINKSYS RE6500 操作系统命令注入漏洞（CNNVD-202012-1569）**

Belkin LINKSYS RE6500 是美国 Belkin 公司的一款无线路由器。

Belkin LINKSYS RE6500 devices 1.0.012.001 之前版本存在操作系统命令注入漏洞，该漏洞允许远程攻击者可利用该漏洞通过 shell 元字符在 goform setSysAdm 页面上执行任意命令或设置新密码。

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://www.linksys.com/us/support-article?articleNum=148460

**5. Google Android 缓冲区错误漏洞（CNNVD-202012-556）**

Google Android 是美国谷歌（Google）和开放手持设备联盟（简称 oha）的一套以 Linux 为基础的开源操作系统。

Google Android Pixel 存在安全漏洞,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://source.android.com/security/bulletin/2020-12-01

**6. Siemens LOGO! 8 BM 访问控制错误漏洞（CNNVD-202012-695）**

Siemens LOGO! 8 BM 是德国西门子（Siemens）公司的一个用于工业环境，用于 Windows 平台的编程软件。

Siemens LOGO! 8 BM 存在访问控制错误漏洞，该漏洞源于能够访问特定服务的攻击者可以在没有授权的情况下获得对所有服务的完全访问权。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://cert-portal.siemens.com/productcert/txt/ssa-480824.txt

**7. Adrem Netcrunch 信任管理问题漏洞（CNNVD-202012-1191）**

Adrem Netcrunch 是美国 Adrem 公司的一个设备监控软件。该软件基于 SNMP 源、Windows 事件日志和 Syslog 服务器等，可对 Windows、Linux、Mac OS X、BSD、NetWare 和 SNMP 设备进行监控。

AdRem NetCrunch 10.6.0.4587 存在信任管理问题漏洞，攻击者可利用该漏洞破解加密保护机制。

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.adremsoft.com/

**8. Cisco Jabber 输入验证错误漏洞（CNNVD-202012-852）**

Cisco Jabber 是美国思科（Cisco）公司的一套统一通信客户端解决方案。该方案提供了在线状态显示、即时消息、语音等功能。

Cisco Jabber 中存在输入验证错误漏洞，该漏洞源于邮件内容验证不正确引起的。攻击者可以通过向受影响的软件发送特制的 XMPP 消息来利用漏洞，通过与目标用户消息交互，攻击者可以在 Jabber 消息窗口界面内注入任意脚本代码。成功利用该漏洞可能使攻击者利用运行 Cisco Jabber 客户端软件的用户帐户的特权，使 MacOS 或 Windows 平台上的应用程序在目标系统上执行任意程序，导致任意代码执行。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-jabber-ZktzjpgO

### 1.4.2 高危漏洞实例

本月高危漏洞共 499 个，其中重点漏洞实例如表 6 所示。

表 6　2020 年 12 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-202012-1095 | Bitbucket | Bitbucket Keysight SQL 注入漏洞（CNNVD-202012-1095） |
| | | CNNVD-202012-1009 | Gallagher Group | |
| | | CNNVD-202012-1983 | HGiga | |
| | | CNNVD-202012-1398 | Mitel | |
| | | CNNVD-202012-984 | OpenAsset | |
| | | CNNVD-202012-1571 | PhpList | |
| | | CNNVD-202012-1426 | Phpgurukul | |
| | | CNNVD-202012-066 | Prestashop | |
| | | CNNVD-202012-713 | Siemens | |
| | | CNNVD-202012-1504 | Steedos | |
| | | CNNVD-202012-1019 | 个人开发者 | |
| | | CNNVD-202012-705 | | |
| | | CNNVD-202012-1982 | 恒基 | |
| 2 | 代码问题 | CNNVD-202012-1784 | 1E | 多款 Schneider Electric 产 |

| | | | | |
|---|---|---|---|---|
| | | CNNVD-202012-1754 | | 品代码问题漏洞（CNNVD-202012-820） |
| | | CNNVD-202012-1464 | ABB | |
| | | CNNVD-202012-730 | Adobe | |
| | | CNNVD-202012-736 | | |
| | | CNNVD-202012-1625 | Automattic | |
| | | CNNVD-202012-062 | Check Point | |
| | | CNNVD-202012-087 | Cloudbees | |
| | | CNNVD-202012-1400 | EPSON | |
| | | CNNVD-202012-1285 | FasterXML | |
| | | CNNVD-202012-1270 | | |
| | | CNNVD-202012-1010 | Gallagher Group | |
| | | CNNVD-202012-1592 | Gobby 团队 | |
| | | CNNVD-202012-1608 | HedgeDoc | |
| | | CNNVD-202012-1501 | Jaws 团队 | |
| | | CNNVD-202012-1499 | | |
| | | CNNVD-202012-387 | Kaspersky | |
| | | CNNVD-202012-1135 | Linux 基金会,Cambridge 大学 | |
| | | CNNVD-202012-394 | Moddable | |
| | | CNNVD-202012-962 | Mout 团队 | |
| | | CNNVD-202012-1474 | Nanosystems | |
| | | CNNVD-202012-932 | Netflix | |
| | | CNNVD-202012-1544 | Openbsd 组织 | |
| | | CNNVD-202012-757 | Palo Alto Networks | |
| | | CNNVD-202012-1510 | Projectworldsofficial 社区 | |
| | | CNNVD-202012-1503 | Redisgraph 社区 | |
| | | CNNVD-202012-1771 | Rockwell Automation | |
| | | CNNVD-202012-1772 | | |
| | | CNNVD-202012-1570 | Rust 社区 | |
| | | CNNVD-202012-822 | Schneider Electric | |
| | | CNNVD-202012-820 | | |
| | | CNNVD-202012-823 | | |
| | | CNNVD-202012-825 | | |
| | | CNNVD-202012-821 | | |
| | | CNNVD-202012-1143 | Sourcecodester | |
| | | CNNVD-202012-1377 | Tangro | |
| | | CNNVD-202012-1212 | Trend Micro | |
| | | CNNVD-202012-941 | Western Digital | |
| | | CNNVD-202012-1083 | XStream 团队 | |
| | | CNNVD-202012-1637 | Zammad | |

| | | | | |
|---|---|---|---|---|
| | | CNNVD-202012-1008 | Zyxel | |
| | | CNNVD-202012-1194 | 个人开发者 | |
| | | CNNVD-202012-1602 | | |
| | | CNNVD-202012-781 | | |
| | | CNNVD-202012-1183 | | |
| | | CNNVD-202012-1276 | | |
| | | CNNVD-202012-091 | | |
| **3** | 授权问题 | CNNVD-202012-1465 | ABB | 多款 Microsoft Windows 产品授权问题漏洞（CNNVD-202012-692） |
| | | CNNVD-202012-1473 | | |
| | | CNNVD-202012-1462 | | |
| | | CNNVD-202012-1012 | Citrix Systems | |
| | | CNNVD-202012-094 | Cloudbees | |
| | | CNNVD-202012-1472 | D-link | |
| | | CNNVD-202012-1471 | | |
| | | CNNVD-202012-1306 | Emerson | |
| | | CNNVD-202012-955 | Frappe 团队 | |
| | | CNNVD-202012-1011 | Gallagher Group | |
| | | CNNVD-202012-1228 | Huawei | |
| | | CNNVD-202012-760 | IBM | |
| | | CNNVD-202012-998 | Macally | |
| | | CNNVD-202012-1275 | Magic Pro | |
| | | CNNVD-202012-862 | Medtronic | |
| | | CNNVD-202012-692 | Microsoft | |
| | | CNNVD-202012-1218 | NZXT | |
| | | CNNVD-202012-068 | National Instruments | |
| | | CNNVD-202012-1745 | Netgear | |
| | | CNNVD-202012-937 | Schneider Electric | |
| | | CNNVD-202012-696 | Siemens | |
| | | CNNVD-202012-1196 | SolarWinds | |
| | | CNNVD-202012-844 | Symantec | |
| | | CNNVD-202012-1550 | Terramaster | |
| | | CNNVD-202012-2021 | Wordpress 基金会 | |
| | | CNNVD-202012-1835 | 个人开发者 | |
| | | CNNVD-202012-789 | | |
| | | CNNVD-202012-774 | | |
| | | CNNVD-202012-077 | | |
| | | CNNVD-202012-097 | | |
| **4** | 操作系统命令注入 | CNNVD-202012-1580 | Belkin | MailSherlock 操作系统命令注入漏洞（CNNVD-202012-1981） |
| | | CNNVD-202012-1466 | D-link | |
| | | CNNVD-202012-1424 | Gohugoio 社区 | |
| | | CNNVD-202012-1981 | HGiga | |

| | | | | |
|---|---|---|---|---|
| | | CNNVD-202012-987 | Nec Platforms | |
| | | CNNVD-202012-1219 | SolarWinds | |
| | | CNNVD-202012-1182 | 个人开发者 | |
| **5** | 缓冲区错误 | CNNVD-202012-1539 | ARM | Microsoft Edge 缓冲区错误漏洞（CNNVD-202012-583） |
| | | CNNVD-202012-654 | Altran EESY Belgium 社区 | |
| | | CNNVD-202012-1111 | Apple | |
| | | CNNVD-202012-1187 | Dell | |
| | | CNNVD-202012-651 | FNET 组织 | |
| | | CNNVD-202012-1559 | FOO 组织 | |
| | | CNNVD-202012-1582 | GNU 社区 | |
| | | CNNVD-202012-462 | Google | |
| | | CNNVD-202012-550 | | |
| | | CNNVD-202012-539 | | |
| | | CNNVD-202012-574 | | |
| | | CNNVD-202012-830 | | |
| | | CNNVD-202012-1152 | | |
| | | CNNVD-202012-528 | | |
| | | CNNVD-202012-829 | | |
| | | CNNVD-202012-459 | | |
| | | CNNVD-202012-464 | | |
| | | CNNVD-202012-465 | | |
| | | CNNVD-202012-552 | | |
| | | CNNVD-202012-1494 | HCL | |
| | | CNNVD-202012-1177 | Huawei | |
| | | CNNVD-202012-1185 | Infraware | |
| | | CNNVD-202012-1523 | Microsoft | |
| | | CNNVD-202012-583 | | |
| | | CNNVD-202012-406 | Mitsubishi Electric | |
| | | CNNVD-202012-395 | Moddable | |
| | | CNNVD-202012-1138 | Mozilla 基金会 | |
| | | CNNVD-202012-034 | | |
| | | CNNVD-202012-1747 | Netgear | |
| | | CNNVD-202012-1789 | | |
| | | CNNVD-202012-1741 | | |
| | | CNNVD-202012-1349 | Treck | |
| | | CNNVD-202012-1348 | | |
| | | CNNVD-202012-096 | Wecon Technologies | |
| | | CNNVD-202012-020 | X.org | |
| | | CNNVD-202012-646 | 个人开发者 | |
| | | CNNVD-202012-647 | | |

| | | | | |
|---|---|---|---|---|
| | | CNNVD-202012-664 | | |
| | | CNNVD-202012-665 | | |
| | | CNNVD-202012-418 | | |
| | | CNNVD-202012-1556 | | |
| | | CNNVD-202012-652 | | |
| | | CNNVD-202012-640 | | |
| | | CNNVD-202012-044 | | |
| | | CNNVD-202012-639 | | |
| **6** | 访问控制错误 | CNNVD-202012-003 | Kia | WordPress Plugin secure-file-manager 访问控制错误漏洞（CNNVD-202012-996） |
| | | CNNVD-202012-729 | Microsoft | |
| | | CNNVD-202012-716 | | |
| | | CNNVD-202012-1743 | Netgear | |
| | | CNNVD-202012-648 | Plum | |
| | | CNNVD-202012-725 | Schneider Electric | |
| | | CNNVD-202012-017 | | |
| | | CNNVD-202012-021 | | |
| | | CNNVD-202012-1436 | Stratodesk | |
| | | CNNVD-202012-1546 | Terramaster | |
| | | CNNVD-202012-996 | WordPress 基金会 | |
| | | CNNVD-202012-1895 | Wordpress 基金会 | |
| | | CNNVD-202012-1449 | ZTE | |
| | | CNNVD-202012-447 | 个人开发者 | |
| | | CNNVD-202012-1977 | 全景 | |
| **7** | 资源管理错误 | CNNVD-202012-801 | Adobe | Red Hat Enterprise Linux 资源管理错误漏洞（CNNVD-202012-064） |
| | | CNNVD-202012-764 | Artifex Software | |
| | | CNNVD-202012-1518 | Bitcoinsv 协会 | |
| | | CNNVD-202012-1524 | | |
| | | CNNVD-202012-1526 | | |
| | | CNNVD-202012-033 | Cloud Foundry 基金会 | |
| | | CNNVD-202012-060 | Eipstackgroup | |
| | | CNNVD-202012-1294 | F5 | |
| | | CNNVD-202012-794 | Foxit | |
| | | CNNVD-202012-796 | | |
| | | CNNVD-202012-793 | | |
| | | CNNVD-202012-803 | | |
| | | CNNVD-202012-469 | Google | |
| | | CNNVD-202012-545 | | |
| | | CNNVD-202012-409 | | |
| | | CNNVD-202012-549 | | |
| | | CNNVD-202012-778 | Linux 基金会 | |
| | | CNNVD-202012-599 | Microsoft | |

| | | | | |
|---|---|---|---|---|
| | | CNNVD-202012-964 | Npm | |
| | | CNNVD-202012-049 | Phoenix Contact | |
| | | CNNVD-202012-064 | Red Hat | |
| | | CNNVD-202012-682 | Systran | |
| | | CNNVD-202012-1645 | 个人开发者 | |
| | | CNNVD-202012-446 | | |
| | | CNNVD-202012-030 | | |
| | | CNNVD-202012-978 | | |
| | | CNNVD-202012-1414 | | |
| **8** | 输入验证错误 | CNNVD-202012-092 | Allen Bradley | Apple Macos Server 输入验证错误漏洞（CNNVD-202012-1055） |
| | | CNNVD-202012-1055 | Apple | |
| | | CNNVD-202012-1578 | Belkin | |
| | | CNNVD-202012-1107 | D-link | |
| | | CNNVD-202012-1105 | | |
| | | CNNVD-202012-100 | Ec-cube | |
| | | CNNVD-202012-455 | Google | |
| | | CNNVD-202012-555 | | |
| | | CNNVD-202012-1648 | Hcl Technologies | |
| | | CNNVD-202012-851 | Host Engineering | |
| | | CNNVD-202012-835 | IBM | |
| | | CNNVD-202012-414 | ImageMagick Studio | |
| | | CNNVD-202012-856 | Medtronic | |
| | | CNNVD-202012-626 | Microsoft | |
| | | CNNVD-202012-1405 | Mitel Networks | |
| | | CNNVD-202012-1482 | Odoo | |
| | | CNNVD-202012-1612 | Open Source Matters | |
| | | CNNVD-202012-977 | Openasset | |
| | | CNNVD-202012-859 | Schneider Electric | |
| | | CNNVD-202012-718 | Siemens | |
| | | CNNVD-202012-1304 | Smilegate | |
| | | CNNVD-202012-1169 | Weseek | |
| | | CNNVD-202012-1104 | 个人开发者 | |
| | | CNNVD-202012-657 | | |
| | | CNNVD-202012-662 | | |
| | | CNNVD-202012-655 | | |
| | | CNNVD-202012-658 | | |
| | | CNNVD-202012-1425 | | |
| | | CNNVD-202012-1031 | | |
| | | CNNVD-202012-1001 | | |
| | | CNNVD-202012-670 | | |

| | | | | |
|---|---|---|---|---|
| | | CNNVD-202012-643 | | |
| | | CNNVD-202012-669 | | |
| | | CNNVD-202012-666 | | |
| | | CNNVD-202012-926 | | |
| | | CNNVD-202012-1966 | 恒基 | |

**1. Bitbucket Keysight SQL 注入漏洞（CNNVD-202012-1095）**

Bitbucket Keysight 是 Bitbucket 组织的一个可用于 Atlassian 产品的数据库连接插件。

Keysight Database Connector plugin before 1.5.0 存在 SQL 注入漏洞，该漏洞源于恶意用户可以绕过访问控制，使用保存的数据库连接配置文件向保存的数据库连接提交任意 SQL 语句。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://bitbucket.org/keysight/keysight-plugins-for-atlassian-products/wiki/Confluence%20Plugins/Database%20Plugin

**2. 多款 Schneider Electric 产品代码问题漏洞（CNNVD-202012-820）**

Schneider Electric Modicon M580 等都是法国施耐德电气（Schneider Electric）公司的产品。Schneider Electric Modicon M580 是一款可编程自动化控制器。Schneider Electric Modicon Premium 是一款用于离散或过程应用的大型可编程逻辑控制器（PLC）。Schneider Electric Modicon Quantum 是一款用于过程应用、高可用性和安全解决方案的大型可编程逻辑控制器（PLC）。

多款 Schneider Electric Modicon 产品存在安全漏洞，攻击者可利用该漏洞使设备拒绝服务。以下产品或版本受到影响：Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & M

odicon Premium。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.se.com/ww/en/download/document/SEVD-2020-343-08/

**3. 多款 Microsoft Windows 产品授权问题漏洞**

**（CNNVD-202012-692）**

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

Microsoft Windows 存在网络连接服务权限提升漏洞,目前尚无此漏洞的相关信息，请随时关注 CNNVD 或厂商公告。以下产品及型号受到影响：Windows Server version 20H2 (Server Core Installation)、Windows Server version 2004 (Server Core installation)、Windows Server version 1909 (Server Core installation)、Windows Server version 1903 (Server Core installation)、Windows Server 2019 (Server Core installation)、Windows Server 2019、Windows Server 2016 (Server Core installation)、Windows Server 2016、Windows Server 2012 R2 (Server Core installation)、Windows Server 2012 R2、Windows Server 2012 (Server Core installation)Windows Server 2012、Windows RT 8.1、Windows 8.1 for x64-based systems、Windows 8.1 for 32-bit systems、Windows 10 for x64-based Systems、Windows 10 for 32-bit Systems、Windows 10 Version 20H2 for x64-based Systems、Windows 10 Version 20H2 for ARM64-based Systems、Wi

ndows 10 Version 20H2 for 32-bit Systems、Windows 10 Version 2004 for x64-based Systems、Windows 10 Version 2004 for ARM64-based Systems、Windows 10 Version 2004 for 32-bit Systems、Windows 10 Version 1909 for x64-based Systems、Windows 10 Version 1909 for ARM64-based Systems、Windows 10 Version 1909 for 32-bit Systems、Windows 10 Version 1903 for x64-based Systems、Windows 10 Version 1903 for ARM64-based Systems、Windows 10 Version 1903 for 32-bit Systems、Windows 10 Version 1809 for x64-based Systems、Windows 10 Version 1809 for ARM64-based Systems、Windows 10 Version 1809 for 32-bit Systems、Windows 10 Version 1803 for x64-based Systems、Windows 10 Version 1803 for ARM64-based Systems、Windows 10 Version 1803 for 32-bit Systems、Windows 10 Version 1607 for x64-based Systems、Windows 10 Version 1607 for 32-bit Systems。

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/zh-CN/vulnerability/CVE-2020-17092

**4. MailSherlock 操作系统命令注入漏洞（CNNVD-202012-1981）**

MailSherlock 是一套企业邮件审核系统。

HGiga MailSherlock 存在安全漏洞，该漏洞源于不能正确地验证特定的参数。攻击者可利用该漏洞远程发起命令注入攻击，并执行系统的任意命令。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.twcert.org.tw/en/cp-139-4264-f10f4-2.html

**5. Microsoft Edge 缓冲区错误漏洞（CNNVD-202012-583）**

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 Edge HTML 存在安全漏洞，攻击者可利用该漏洞来运行代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://msrc.microsoft.com/update-guide/zh-CN/vulnerability/CVE-2020-17131

**6. WordPress Plugin secure-file-manager 访问控制错误漏洞（CNNVD-202012-996）**

WordPress 是 WordPress（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 secure-file-manager plugin through 2.5 版本存在访问控制错误漏洞，该漏洞源于 vendor/elfinder/php/connector.minimal.php 加载 elfinder 代码没有适当的访问控制。任何经过身份验证的用户都可以运行 elFinder upload 命令来实现远程代码执行。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://wordpress.org/plugins/easy-wp-smtp/#developers

**7. Red Hat Enterprise Linux 资源管理错误漏洞**

**（CNNVD-202012-064）**

Red Hat Enterprise Linux 是美国红帽（Red Hat）公司的面向企业用户的 Linux 操作系统。

Red Hat Enterprise Linux 存在资源管理错误漏洞，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，导致相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://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=c1f6e3c818dd734c30f6a7eeebf232ba2cf3181d

**8. Apple Macos Server 输入验证错误漏洞（CNNVD-202012-1055）**

Apple Macos Server 是美国 Apple 公司的一款服务端版本的操作系统。

macOS Server 5.11 之前版本存在输入验证错误漏洞，该漏洞源于处理恶意制作的 URL 可能导致开放重定向或跨站点脚本描述。

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/zh-cn/HT211932

## 二、接报漏洞情况

本月接报漏洞 58601 个，其中信息技术产品漏洞（通用型漏洞）192 个，网络信息系统漏洞（事件型漏洞）58409 个。

表 7 2020 年 12 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 | 46546 |
| 2 | 上海斗象信息科技有限公司 | 10011 |
| 3 | 河南听潮盛世信息技术有限公司 | 737 |
| 4 | 北京奇虎科技有限公司 | 240 |
| 5 | 山东云天安全技术有限公司 | 210 |
| 6 | 山东华鲁科技发展股份有限公司 | 157 |
| 7 | 北京天地和兴科技有限公司 | 103 |
| 8 | 西安交大捷普网络科技有限公司 | 100 |
| 9 | 北京山石网科信息技术有限公司 | 84 |
| 10 | 山东新潮信息技术有限公司 | 69 |
| 11 | 浙江大华技术股份有限公司 | 59 |
| 12 | 北京计算机技术及应用研究所 | 32 |
| 13 | 北京数字观星科技有限公司 | 30 |
| 14 | 内蒙古奥创科技有限公司 | 25 |
| 15 | 远江盛邦（北京）网络安全科技股份有限公司 | 20 |
| 16 | 杭州海康威视数字技术股份有限公司 | 18 |
| 17 | 广州竞远安全技术股份有限公司 | 16 |
| 18 | 广东东福信息技术有限公司 | 15 |
| 19 | 新华三技术有限公司 | 15 |
| 20 | 新疆海狼科技有限公司 | 12 |
| 21 | 北京华云安信息技术有限公司 | 10 |
| 22 | 博智安全科技股份有限公司 | 10 |
| 23 | 上海安识网络科技有限公司 | 10 |

| | | |
|---|---|---|
| 24 | 北京天融信网络安全技术有限公司 | 8 |
| 25 | 杭州美创科技有限公司 | 8 |
| 26 | 清华大学网络科学与网络空间研究院 | 8 |
| 27 | 北京优炫软件股份有限公司 | 7 |
| 28 | 杭州默安科技有限公司 | 7 |
| 29 | 北京网御星云信息技术有限公司 | 6 |
| 30 | 绿盟科技集团股份有限公司安全研究部 | 5 |
| 31 | 个人 | 4 |
| 32 | 中国科学院软件研究所 | 4 |
| 33 | [苏州极光无限信息技术有限公司] | 3 |
| 34 | 北京威努特技术有限公司 | 3 |
| 35 | 北京智游网安科技有限公司 | 3 |
| 36 | 恒安嘉新（北京）科技股份公司 | 3 |
| 37 | 浪潮电子信息产业股份有限公司 | 3 |
| 38 | 苏州极光无限信息技术有限公司 | 3 |
| 39 | 中兴通讯 | 3 |
| 40 | [北京山石网科信息技术有限公司] | 2 |
| 41 | 北京启明星辰信息安全技术有限公司 | 2 |
| 42 | 北京市星阑科技有限公司 | 2 |
| 43 | 恒安嘉新(北京)科技股份公司 | 2 |
| 44 | 四川虹微技术有限公司 | 2 |
| 45 | 亚信科技（成都）有限公司 | 2 |
| 46 | 安徽长泰信息安全服务有限公司 | 1 |

| | | |
|---|---|---|
| 47 | 成都新潮传媒集团 | 1 |
| 48 | 湖南汽车工程职业学校 | 1 |
| 49 | 绿盟科技集团股份有限公司工业物联网安全实验室 | 1 |
| 50 | 信息工程大学 | 1 |
| 51 | 中国电子科技网络信息安全有限公司 | 1 |
| 报送总计 | | 58601 |

# 三、重大漏洞预警

## 3.1 Apache Struts 2 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 Apache Struts2 S2-061 远程代码执行漏洞（CNNVD-202012-449、CVE-2020-17530）情况的报送。成功利用漏洞的攻击者可以在目标系统执行恶意代码。Apache Struts 2.0.0 - 2.5.25 版本均受此漏洞影响。目前，Apache 官方已经发布了版本更新修复了该漏洞。建议用户及时确认产品版本，尽快采取修补措施。

### .漏洞介绍

Apache Struts 是美国阿帕奇（Apache）基金会的一个开源项目，是一套用于创建企业级 Java Web 应用的开源 MVC 框架，主要提供两个版本框架产品，Struts 1 和 Struts 2。

洞源于 Apache Struts2 在某些标签属性中使用 OGNL 表达式时，因为没有做内容过滤，导致攻击者传入精心构造的请求时，可以造成 OGNL 二次解析，执行指定的恶意代码。

**.危害影响**

成功利用漏洞的攻击者可以在目标系统执行恶意代码。Apache Struts 2.0.0 - 2.5.25 版本均受此漏洞影响。

**.修复建议**

目前，Apache 官方已经发布了版本更新修复了该漏洞。建议用户及时确认产品版本，尽快采取修补措施。Apache 官方更新链接如下：

http://struts.apache.org/download.cgi

## 3.2 微软多个安全漏洞的的预警

近日，微软官方发布了多个安全漏洞的公告，包括 Microsoft Exchange Server 安全漏洞（CNNVD-202012-615、CVE-2020-17117）、Microsoft SharePoint 安全漏洞（CNNVD-202012-620、CVE-2020-17118）、Microsoft Excel 安全漏洞（CNNVD-202012-616、CVE-2020-17122）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 12 月 9 日，微软发布了 2020 年 12 月份安全更新，共 58 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、ChakraCore、Office 办公套件、Exchange Server、Azure、Visual Studio 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、Microsoft Exchange Server 安全漏洞（CNNVD-202012-615、CVE-2020-17132 ）（ CNNVD-202012-615 、 CVE-2020-17117 ）（CNNVD-202012-606、CVE-2020-17142）

漏洞简介：由于 Exchange 对 cmdlet 参数的验证不正确，会触发一个 Microsoft Exchange 服务器中的远程代码执行漏洞。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。

2、Microsoft SharePoint 安全漏洞（ CNNVD-202012-620 、CVE-2020-17118）（CNNVD-202012-617、CVE-2020-17121）

漏洞简介：SharePoint 中存在一个安全漏洞。经过身份验证的攻击者通过发送特制请求包，可在 SharePoint Web 应用中执行任意.NET 代码。

3、Microsoft Excel 安全漏洞（CNNVD-202012-616、CVE-2020-17122）（CNNVD-202012-584、CVE-2020-17127）（CNNVD-202012-586、CVE-2020-17129）

漏洞简介：Microsoft Excel 中存在安全漏洞。当 Microsoft Excel 软件无法正确处理内存中的对象时，该软件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当前用户的上下文中运行任意代码。

4、Microsoft PowerPoint 安全漏洞（CNNVD-202012-592、CVE-2020-17124）

漏洞简介：由于 Microsoft SharePoint 对用户输入验证不足，攻击者可以输入一些精心构造的数据，造成内存破坏，从而导致远程代码执行。

5、Microsoft Windows Hyper-V 安全漏洞（CNNVD-202012-687、CVE-2020-17095）

漏洞简介：Microsoft Windows Hyper-V 中存在安全漏洞。当主机服务器上的 Windows Hyper-V 无法正确验证来宾操作系统上经身份验证的用户的输入时，存在远程代码执行漏洞。成功利用此漏洞的攻击者可以在主机操作系统上执行任意代码。

6、Microsoft Edge 安全漏洞（CNNVD-202012-583、CVE-2020-17131）

漏洞简介：Microsoft Edge 存在一个安全漏洞，攻击者可利用该漏洞可以远程执行恶意代码。

由于此次更新，微软并没有透露太多漏洞详情，请用户自行到官方网站查询，官方地址：

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

**.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