# 北京师范大学网络信息安全通告

## 2019 年 9 月报告

北京师范大学信息网络中心

2019 年 10 月

# 目录

# 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，2019 年 9 月份新增安全漏洞共 1377 个，从厂商分布来看，Google 公司产品的漏洞数量最多，共发布 94 个；从漏洞类型来看，跨站脚本类的漏洞占比最大，达到 16.34%。本月新增漏洞中，超危漏洞 143 个、高危漏洞 460 个、中危漏洞 736 个、低危漏洞 38 个，相应修复率分别为 76.92%、84.13%、76.90%以及 89.47%。合计 1097 个漏洞已有修复补丁发布，本月整体修复率 79.67%。

截至 2019 年 9 月 30 日，CNNVD 采集漏洞总量已达 133175 个。

### 1.1 漏洞增长概况

2019 年 9 月新增安全漏洞 1377 个，与上月（2264 个）相比减少了 39.18%。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 1551 个。

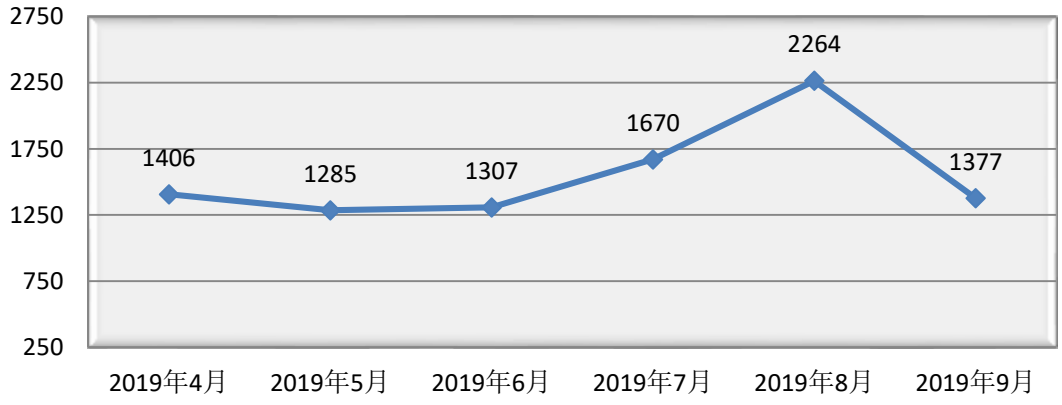


图 1 2019 年 4 月至 2019 年 9 月漏洞新增数量统计图

## 1.2 漏洞分布情况

### 1.2.1 漏洞厂商分布

9 月厂商漏洞数量分布情况如表 1 所示，谷歌公司达到 94 个，占本月漏洞总量的 6.83%。本月 GitLab、Mozilla、苹果等公司的漏洞数量均有所上升，谷歌、微软等厂商的漏洞数量出现较不同程度的下降。

表 1　2019 年 9 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** | 谷歌 | 94 | 6.83% |
| **2** | 微软 | 79 | 5.74% |
| **3** | GitLab | 50 | 3.63% |
| **4** | Qualcomm | 45 | 3.27% |
| **5** | CloudBees | 39 | 2.83% |
| **6** | 思科 | 38 | 2.76% |
| **7** | IBM | 33 | 2.40% |
| **8** | Linux | 30 | 2.18% |
| **9** | Mozilla | 22 | 1.60% |
| **10** | 苹果 | 18 | 1.31% |

### 1.2.2 漏洞产品分布

9 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 49 条，其中桌面操作系统 49 条，服务器操作系统 47 条。本月 Android 漏洞数量最多，共 52 个，占主流操作系统漏洞总量的 12.26%，排名第一。

表 2　2019 年 9 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 | 52 |

| | | |
|---|---|---|
| **2** | Windows 10 | 47 |
| **3** | Windows Server 1803 | 44 |
| **4** | Windows Server 1903 | 43 |
| **5** | Windows Server 2016 | 39 |
| **6** | Windows 8.1 | 33 |
| **7** | Windows 7 | 32 |
| **8** | Windows Rt 8.1 | 32 |
| **9** | Windows Server 2012 | 31 |
| **10** | Windows Server 2008 | 31 |
| **11** | Linux Kernel | 30 |
| **12** | Apple iOS | 10 |

*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

9 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 16.34%。

表 32019 年 9 月漏洞类型统计表

| 序号 | 漏洞类型 | 漏洞数量 | 所占比例 |
|---|---|---|---|
| **1** | 跨站脚本 | 225 | 16.34% |
| **2** | 输入验证错误 | 155 | 11.26% |
| **3** | 缓冲区错误 | 141 | 10.24% |
| **4** | 信息泄露 | 110 | 7.99% |
| **5** | 代码问题 | 87 | 6.32% |
| **6** | 资源管理错误 | 66 | 4.79% |
| **7** | 跨站请求伪造 | 66 | 4.79% |

| | | | |
|---|---|---|---|
| **8** | SQL 注入 | 50 | 3.63% |
| **9** | 授权问题 | 41 | 2.98% |
| **10** | 路径遍历 | 33 | 2.40% |
| **11** | 访问控制错误 | 27 | 1.96% |
| **12** | 注入 | 19 | 1.38% |
| **13** | 信任管理问题 | 14 | 1.02% |
| **14** | 操作系统命令注入 | 12 | 0.87% |
| **15** | 代码注入 | 11 | 0.80% |
| **16** | 竞争条件问题 | 9 | 0.65% |
| **17** | 命令注入 | 9 | 0.65% |
| **18** | 权限许可和访问控制问题 | 8 | 0.58% |
| **19** | 安全特征问题 | 6 | 0.44% |
| **20** | 数据伪造问题 | 5 | 0.36% |
| **21** | 加密问题 | 3 | 0.22% |
| **22** | 数字错误 | 3 | 0.22% |
| **23** | 环境问题 | 2 | 0.15% |
| **24** | 格式化字符串错误 | 1 | 0.07% |
| **25** | 后置链接 | 1 | 0.07% |
| **26** | 配置错误 | 1 | 0.07% |
| **27** | 日志信息泄露 | 1 | 0.07% |

### 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。9 月漏洞危害等级分布如图 2 所示，其中超危漏洞 143 条，占本月漏洞总数的 10.38%。

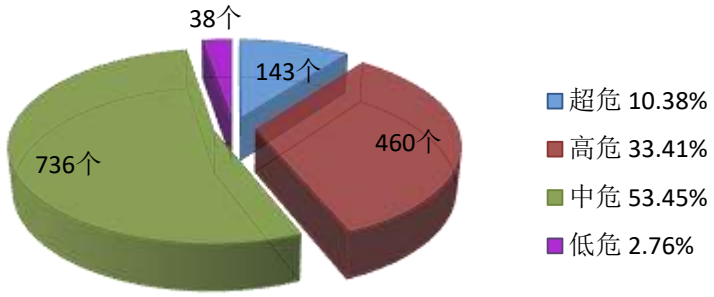


图 2　2019 年 9 月漏洞危害等级分布

## 1.3 漏洞修复情况

### 1.3.1　整体修复情况

9 月漏洞修复情况按危害等级进行统计见图 3。其中低漏洞修复率最高，达到 89.47%，中危漏洞修复率最低，比例为 76.90%。与上月相比，本月低危漏洞修复率有所上升，超、高、中危漏洞修复率有所下降。总体来看，本月整体修复率下降，由上月的 85.29%下降至本月的 79.67%。

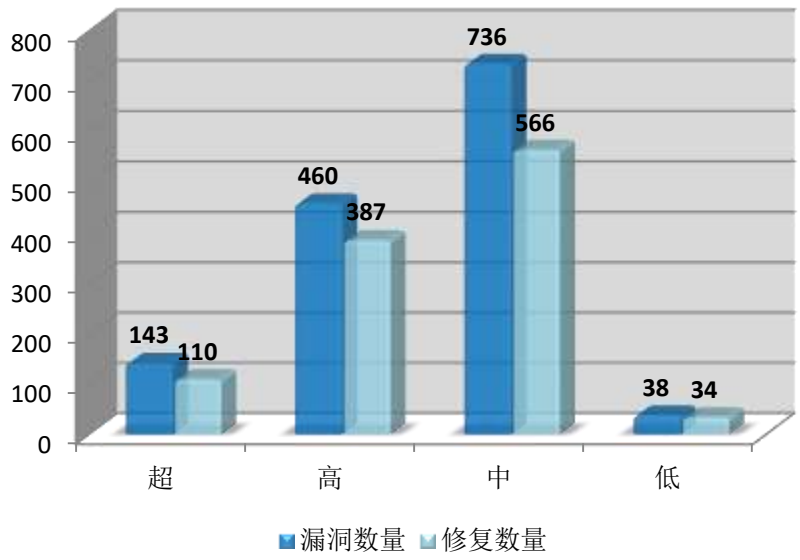


图 3　2019 年 9 月漏洞修复数量统计

### 1.3.2 厂商修复情况

9 月漏洞修复情况按漏洞数量前十厂商进行统计，其中谷歌、微软、GitLab 等十个厂商共 448 条漏洞，占本月漏洞总数的 32.53%，漏洞修复率为 97.54%，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，其中微软、GitLab、Qualcomm、思科等公司本月漏洞修复率均为 100%，共 485 条漏洞已全部修复。

表 4　2019 年 9 月厂商修复情况统计表

| 序号 | 厂商名称 | 漏洞数量 | 修复数量 | 修复率 |
|---|---|---|---|---|
| **1** | 谷歌 | 94 | 93 | 98.94% |
| **2** | 微软 | 79 | 79 | 100.00% |
| **3** | GitLab | 50 | 50 | 100.00% |
| **4** | Qualcomm | 45 | 45 | 100.00% |
| **5** | CloudBees | 39 | 29 | 74.36% |
| **6** | 思科 | 38 | 38 | 100.00% |
| **7** | IBM | 33 | 33 | 100.00% |
| **8** | Linux | 30 | 30 | 100.00% |
| **9** | Mozilla | 22 | 22 | 100.00% |
| **10** | 苹果 | 18 | 18 | 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 143 个，其中重要漏洞实例如表 5 所示。

表 5　2019 年 9 月超危漏洞实例

| 序号 | 漏洞类型 | CNNVD 编号 | 厂商 | 漏洞实例 |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| 1 | 资源管理错误 | CNNVD-201909-602 | Google | Google Chrome Media 资源管理错误漏洞（CNNVD-201909-602） |
| | | CNNVD-201909-836 | Aspose | |
| | | CNNVD-201909-846 | | |
| 2 | 信息泄露 | CNNVD-201909-1011 | F5 | Microsoft DirectWrite 信息泄露漏洞（CNNVD-201909-479） |
| | | CNNVD-201909-968 | | |
| | | CNNVD-201909-479 | Microsoft | |
| | | CNNVD-201909-153 | Cisco | |
| 3 | 信任管理问题 | CNNVD-201909-650 | Bosch | Schneider Electric APC UPS Network Management Card 2 信任管理问题漏洞（CNNVD-201909-814） |
| | | CNNVD-201909-814 | Schneider Electric | |
| 4 | 输入验证错误 | CNNVD-201909-1053 | 中兴 | ZTE ZXV10 B860A 输入验证错误漏洞（CNNVD-201909-1053） |
| | | CNNVD-201909-1094 | NetApp | |
| | | CNNVD-201909-123 | Qualcomm | |
| | | CNNVD-201909-156 | | |
| | | CNNVD-201909-474 | Microsoft | |
| | | CNNVD-201909-579 | Apache | |
| | | CNNVD-201909-594 | | |
| | | CNNVD-201909-633 | CloudBees | |
| | | CNNVD-201909-634 | | |
| | | CNNVD-201909-876 | TIBCO Software | |
| | | CNNVD-201909-878 | | |
| 5 | 授权问题 | CNNVD-201909-269 | Apache | eQ-3 Homematic CCU3 和 eQ-3 HomeMatic CCU2 授权问题漏洞（CNNVD-201909-844） |
| | | CNNVD-201909-454 | Couchbase | |
| | | CNNVD-201909-642 | Tripp Lite | |
| | | CNNVD-201909-833 | 研华 | |
| | | CNNVD-201909-844 | eQ-3 | |
| | | CNNVD-201909-886 | Dell | |

| | | | | |
|---|---|---|---|---|
| **6** | 缓冲区错误 | CNNVD-201909-1080 | wolfSSL | 3S-Smart Software Solutions CODESYS V3 web server 缓冲区错误漏洞（CNNVD-201909-658） |
| | | CNNVD-201909-1075 | Linux | |
| | | CNNVD-201909-180 | | |
| | | CNNVD-201909-202 | | |
| | | CNNVD-201909-258 | Facebook | |
| | | CNNVD-201909-431 | 研华 | |
| | | CNNVD-201909-658 | 3S-Smart Software Solutions | |
| | | CNNVD-201909-677 | Race River | |
| | | CNNVD-201909-860 | 大华 | |
| **7** | 访问控制错误 | CNNVD-201909-083 | CA | Knowage 访问控制错误漏洞（CNNVD-201909-227） |
| | | CNNVD-201909-1180 | Cisco | |
| | | CNNVD-201909-227 | Knowage | |
| | | CNNVD-201909-366 | GitLab | |
| | | CNNVD-201909-435 | Adobe | |
| **8** | 代码注入 | CNNVD-201909-453 | Couchbase | Advantech WebAccess 代码注入漏洞（CNNVD-201909-843） |
| | | CNNVD-201909-843 | 研华 | |
| **9** | 代码问题 | CNNVD-201909-590 | Apache | Apache Tapestry 代码问题漏洞（CNNVD-201909-758） |
| | | CNNVD-201909-758 | | |
| | | CNNVD-201909-784 | Code42 Software | |
| | | CNNVD-201909-835 | Schneider Electric | |
| **10** | 操作系统命令注入 | CNNVD-201909-727 | 友讯 | D-Link DNS-320 操作系统命令注入漏洞（CNNVD-201909-727） |

## 1. Google Chrome Media 资源管理错误漏洞（CNNVD-201909-602）

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。

Media 是其中的一个多媒体组件。

Google Chrome 77.0.3865.75 之前版本中的 Media 存在资源管理错误漏洞。远程攻击者可借助特制的网站利用该漏洞在系统上执行任意代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://chromereleases.googleblog.com/2019/09/stable-channel-update-for-desktop.html

**2. Microsoft DirectWrite 信息泄露漏洞（CNNVD-201909-479）**

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。DirectWrite 是其中的一个文本布局和字形渲染 API（应用程序编程接口）。

Microsoft DirectWrite 中存在信息泄露漏洞。攻击者可利用该漏洞获取信息。以下产品及版本受到影响：

- Microsoft Windows 10
- Microsoft Windows 10 版本 1607
- Microsoft Windows 10 版本 1703
- Microsoft Windows 10 版本 1709
- Microsoft Windows 10 版本 1803
- Microsoft Windows 10 版本 1809
- Microsoft Windows 10 版本 1903

- Microsoft Windows 7 SP1
- Microsoft Windows 8.1
- Microsoft Windows RT 8.1
- Microsoft Windows Server 2008 SP2
- Microsoft Windows Server 2008 R2 SP1
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Microsoft Windows Server 版本 1803
- Microsoft Windows Server 版本 1903

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-2019-1245

3. **Schneider Electric APC UPS Network Management Card 2 信任管理问题漏洞（CNNVD-201909-814）**

Schneider Electric APC UPS Network Management Card 2 是法国施耐德电气（Schneider Electric）公司的一款网络管理卡。

Schneider Electric APC UPS Network Management Card 2 AOS v6.5.6 版本中存在信任管理问题漏洞。攻击者可利用该漏洞查看明文形式的远程监控凭证。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.apc.com/salestools/CCON-BFQMXC/CCON-BFQMXC_R0_EN.pdf

4. ZTE ZXV10 B860A 输入验证错误漏洞（CNNVD-201909-1053）

ZTE ZXV10 B860A 是中国中兴通讯（ZTE）公司的一款网络机顶盒。

ZTE ZXV10 B860A 81511329.1008 及之前版本中存在输入验证错误漏洞。攻击者可利用该漏洞控制用户的终端系统。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

http://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1011263

5. eQ-3 Homematic CCU3 和 eQ-3 HomeMatic CCU2 授权问题漏洞（CNNVD-201909-844）

eQ-3 Homematic CCU3 和 eQ-3 HomeMatic CCU2 都是德国 eQ-3 公司的一款智能家居系统的中央控制单元。

eQ-3 Homematic CCU2 2.47.18 之前版本和 eQ-3 Homematic CCU3 3.47.18 之前版本中存在授权问题漏洞。攻击者可借助 HTTP POST 请求利用该漏洞执行代码。

目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：

https://www.eq-3.com/

6. 3S-Smart Software Solutions CODESYS V3 web server 缓冲区错误漏洞（CNNVD-201909-658）

3S-Smart Software Solutions CODESYS V3 web server 是德国

3S-Smart Software Solutions 公司的一款使用在 CODESYS 产品中的 Web 服务器。

3S-Smart Software Solutions CODESYS V3 web server 3.5.14.10 之前版本中存在缓冲区错误漏洞。攻击者可通过发送特制的 http 或 https 请求利用该漏洞造成拒绝服务或执行代码。

目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：

https://www.codesys.com/

**7. Knowage 访问控制错误漏洞（CNNVD-201909-227）**

Knowage 是意大利 Knowage 公司的一套用于在传统资源和大数据系统上进行现代业务分析的开源套件。

Knowage 6.1.1 及之前版本中存在访问控制错误漏洞。攻击者可利用该漏洞绕过访问控制并访问整个应用程序。

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.knowage-suite.com

**8. Advantech WebAccess 代码注入漏洞（CNNVD-201909-843）**

Advantech WebAccess 是中国台湾研华（Advantech）公司的一套基于浏览器架构的 HMI/SCADA 软件。该软件支持动态图形显示和实时数据控制，并提供远程控制和管理自动化设备的功能。

Advantech WebAccess 8.4.1 及之前版本中存在代码注入漏洞。攻击者可利用该漏洞执行远程代码或导致系统崩溃。

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.advantech.com

9. Apache Tapestry 代码问题漏洞（CNNVD-201909-758）

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

Apache Tapestry 5.4.0 版本（包括：betas 版本）至 5.4.3 版本中存在代码问题漏洞。攻击者可利用该漏洞运行恶意的 Java 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://lists.apache.org/thread.html/5173c4eed06e2fca6fd5576ed723ff6bb1711738ec515cb51a04ab24@<users.tapestry.apache.org>

10. D-Link DNS-320 操作系统命令注入漏洞（CNNVD-201909-727）

D-Link DNS-320 是中国台湾友讯（D-Link）公司的一款 NAS（网络附属存储）设备。

D-Link DNS-320 2.05.B10 及之前版本中的 login_mgr.cgi 脚本存在操作系统命令注入漏洞。攻击者可利用该漏洞执行任意命令。

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.dlink.com/

### 1.4.2 高危漏洞实例

本月高危漏洞共 460 个，其中重点漏洞实例如表 6 所示。

表 6　2019 年 9 月高危漏洞实例

| 序号 | 漏洞类型 | CNNVD 编号 | 厂商 | 漏洞实例 |
|---|---|---|---|---|
| 1 | 资源管理错误 | CNNVD-201909-970 | VMware | IBM Cognos Analytics 资源管理错误漏洞（CNNVD-201909-724） |
| | | CNNVD-201909-438 | SAP | |
| | | CNNVD-201909-245 | Red Lion Controls | |

| | | | | |
|---|---|---|---|---|
| | | CNNVD-201909-1352 | Qualcomm | |
| | | CNNVD-201909-162 | | |
| | | CNNVD-201909-163 | | |
| | | CNNVD-201909-170 | | |
| | | CNNVD-201909-035 | Mozilla | |
| | | CNNVD-201909-062 | | |
| | | CNNVD-201909-188 | Linux | |
| | | CNNVD-201909-190 | | |
| | | CNNVD-201909-191 | | |
| | | CNNVD-201909-192 | | |
| | | CNNVD-201909-198 | | |
| | | CNNVD-201909-724 | IBM | |
| | | CNNVD-201909-139 | Google | |
| | | CNNVD-201909-143 | | |
| | | CNNVD-201909-588 | | |
| | | CNNVD-201909-593 | | |
| | | CNNVD-201909-600 | | |
| | | CNNVD-201909-900 | | |
| | | CNNVD-201909-003 | GitLab | |
| | | CNNVD-201909-016 | | |
| | | CNNVD-201909-452 | Couchbase | |
| | | CNNVD-201909-1120 | Cisco | |
| | | CNNVD-201909-1167 | | |
| | | CNNVD-201909-1181 | | |
| | | CNNVD-201909-840 | Aspose | |
| | | CNNVD-201909-427 | Apache | |
| | | CNNVD-201909-442 | Adobe | |

| | | | | |
|---|---|---|---|---|
| 2 | 注入 | CNNVD-201909-005 | GitLab | Cisco Webex Teams 注入漏洞（CNNVD-201909-160） |
| | | CNNVD-201909-160 | Cisco | |
| | | CNNVD-201909-903 | Atlassian | |
| 3 | 信息泄露 | CNNVD-201909-1362 | Western Digital | Bosch Access Professional Edition 信息泄露漏洞（CNNVD-201909-651） |
| | | CNNVD-201909-827 | VMware | |
| | | CNNVD-201909-832 | | |
| | | CNNVD-201909-688 | Siemens | |
| | | CNNVD-201909-432 | SAP | |
| | | CNNVD-201712-819 | Qualcomm | |
| | | CNNVD-201909-462 | Micro Focus | |
| | | CNNVD-201909-810 | | |
| | | CNNVD-201909-815 | | |
| | | CNNVD-201909-1063 | Linux | |
| | | CNNVD-201909-084 | Google | |
| | | CNNVD-201909-006 | GitLab | |
| | | CNNVD-201909-007 | | |
| | | CNNVD-201909-009 | | |
| | | CNNVD-201909-011 | | |
| | | CNNVD-201909-013 | | |
| | | CNNVD-201909-014 | | |
| | | CNNVD-201909-015 | | |
| | | CNNVD-201909-018 | | |
| | | CNNVD-201909-020 | | |
| | | CNNVD-201909-346 | | |
| | | CNNVD-201909-351 | | |
| | | CNNVD-201909-358 | | |
| | | CNNVD-201909-589 | Dell | |

| | | | | |
|---|---|---|---|---|
| | | CNNVD-201909-651 | Bosch | |
| 4 | 信任管理问题 | CNNVD-201909-043 | Dell | Dell EMC Enterprise Copy Data Management 信任管理问题漏洞（CNNVD-201909-043） |
| | | CNNVD-201909-455 | Couchbase | |
| 5 | 输入验证错误 | CNNVD-201909-182 | 乐鑫信息科技 | Cisco IOS XE 输入验证错误漏洞（CNNVD-201909-1162） |
| | | CNNVD-201909-183 | | |
| | | CNNVD-201909-873 | 晶睿通讯 | |
| | | CNNVD-201909-857 | 大华 | |
| | | CNNVD-201909-892 | Valve | |
| | | CNNVD-201909-434 | Siemens | |
| | | CNNVD-201909-441 | SAP | |
| | | CNNVD-201909-114 | Qualcomm | |
| | | CNNVD-201909-120 | Qualcomm | |
| | | CNNVD-201909-122 | | |
| | | CNNVD-201909-124 | | |
| | | CNNVD-201909-126 | | |
| | | CNNVD-201909-127 | | |
| | | CNNVD-201909-144 | | |
| | | CNNVD-201909-151 | | |
| | | CNNVD-201909-155 | | |
| | | CNNVD-201909-158 | | |
| | | CNNVD-201909-166 | | |
| | | CNNVD-201909-172 | | |
| | | CNNVD-201909-174 | | |
| | | CNNVD-201909-175 | | |
| | | CNNVD-201909-031 | Mozilla | |
| | | CNNVD-201909-1064 | Microsoft | |

| | | | | |
|---|---|---|---|---|
| | | CNNVD-201909-420 | | |
| | | CNNVD-201909-424 | | |
| | | CNNVD-201909-428 | | |
| | | CNNVD-201909-482 | | |
| | | CNNVD-201909-483 | | |
| | | CNNVD-201909-486 | | |
| | | CNNVD-201909-492 | | |
| | | CNNVD-201909-498 | | |
| | | CNNVD-201909-520 | | |
| | | CNNVD-201909-522 | | |
| | | CNNVD-201909-532 | | |
| | | CNNVD-201909-533 | | |
| | | CNNVD-201909-534 | | |
| | | CNNVD-201909-564 | McAfee | |
| | | CNNVD-201909-565 | | |
| | | CNNVD-201909-106 | Google | |
| | | CNNVD-201909-133 | | |
| | | CNNVD-201909-1366 | Evernote | |
| | | CNNVD-201909-1153 | Cisco | |
| | | CNNVD-201909-1162 | | |
| | | CNNVD-201909-1169 | | |
| | | CNNVD-201909-1193 | | |
| | | CNNVD-201909-150 | | |
| | | CNNVD-201909-157 | | |
| | | CNNVD-201909-086 | Aruba Networks | |
| | | CNNVD-201909-659 | 3S-Smart Software Solutions | |

| | | | | |
|---|---|---|---|---|
| 6 | 授权问题 | CNNVD-201909-002 | GitLab | GitLab 授权问题漏洞（CNNVD-201909-339） |
| | | CNNVD-201909-017 | | |
| | | CNNVD-201909-339 | | |
| | | CNNVD-201909-140 | Google | |
| | | CNNVD-201909-137 | | |
| | | CNNVD-201909-241 | BD | |
| | | CNNVD-201909-824 | Schneider Electric | |
| 7 | 权限许可和访问控制问题 | CNNVD-201909-108 | Google | Android NVIDIA BootROM 权限许可和访问控制问题漏洞（CNNVD-201909-176） |
| | | CNNVD-201909-142 | | |
| | | CNNVD-201909-176 | | |
| 8 | 命令注入 | CNNVD-201909-1139 | Cisco | Cisco IOS XE 命令注入漏洞（CNNVD-201909-1139） |
| | | CNNVD-201909-1146 | | |
| | | CNNVD-201909-1259 | Netskope | |
| 9 | 路径遍历 | CNNVD-201909-352 | GitLab | 3S-Smart Software Solutions CODESYS V3 web server 路径遍历漏洞（CNNVD-201909-657） |
| | | CNNVD-201909-657 | 3S-Smart Software Solutions | |
| | | CNNVD-201909-764 | Apache | |
| | | CNNVD-201909-898 | Atlassian | |
| 10 | 跨站脚本 | CNNVD-201909-019 | GitLab | Dell EMC Integrated Data Protection Appliance 跨站脚本漏洞（CNNVD-201909-1310） |
| | | CNNVD-201909-069 | Mozilla | |
| | | CNNVD-201909-078 | | |
| | | CNNVD-201909-1310 | Dell | |
| | | CNNVD-201909-655 | 3S-Smart Software Solutions | |
| 11 | 竞争条件问题 | CNNVD-201909-049 | Mozilla | Mozilla Firefox 竞争条件问题漏洞（CNNVD-201909-049） |
| 12 | 缓冲区错 | CNNVD-201909-837 | 研华 | Microsoft Internet |

| | | | | |
|---|---|---|---|---|
| | 误 | CNNVD-201909-471 | 台达电子 | Explorer 缓冲区错误漏洞（CNNVD-201909-1071） |
| | | CNNVD-201909-537 | | |
| | | CNNVD-201909-538 | | |
| | | CNNVD-201909-804 | 华硕 | |
| | | CNNVD-201909-817 | 福昕 | |
| | | CNNVD-201909-821 | | |
| | | CNNVD-201909-825 | | |
| | | CNNVD-201909-270 | Red Lion Controls | |
| | | CNNVD-201909-271 | | |
| | | CNNVD-201909-807 | Red Hat | |
| | | CNNVD-201909-887 | | |
| | | CNNVD-201909-118 | Qualcomm | |
| | | CNNVD-201909-1351 | | |
| | | CNNVD-201909-164 | | |
| | | CNNVD-201909-169 | | |
| | | CNNVD-201909-1258 | Netskope | |
| | | CNNVD-201909-042 | Mozilla | |
| | | CNNVD-201909-1071 | Microsoft | |
| | | CNNVD-201909-399 | | |
| | | CNNVD-201909-400 | | |
| | | CNNVD-201909-401 | | |
| | | CNNVD-201909-405 | | |
| | | CNNVD-201909-406 | | |
| | | CNNVD-201909-409 | | |
| | | CNNVD-201909-429 | | |
| | | CNNVD-201909-476 | | |
| | | CNNVD-201909-477 | | |

| | | | | |
|---|---|---|---|---|
| | | CNNVD-201909-478 | | |
| | | CNNVD-201909-487 | | |
| | | CNNVD-201909-493 | | |
| | | CNNVD-201909-495 | | |
| | | CNNVD-201909-499 | | |
| | | CNNVD-201909-503 | | |
| | | CNNVD-201909-519 | | |
| | | CNNVD-201909-528 | | |
| | | CNNVD-201909-185 | Linux | |
| | | CNNVD-201909-189 | | |
| | | CNNVD-201909-201 | | |
| | | CNNVD-201909-204 | | |
| | | CNNVD-201909-213 | Hanwah Techwin | |
| | | CNNVD-201909-136 | Google | |
| | | CNNVD-201909-138 | | |
| | | CNNVD-201909-146 | | |
| | | CNNVD-201909-601 | | |
| | | CNNVD-201909-064 | EZAutomation | |
| | | CNNVD-201909-070 | | |
| 13 | 代码注入 | CNNVD-201909-436 | SAP | Dell RSA Identity Governance and Lifecycle 和 RSA Via Lifecycle and Governance 代码注入漏洞（CNNVD-201909-585） |
| | | CNNVD-201909-585 | Dell | |
| 14 | 代码问题 | CNNVD-201909-868 | 小米 | Epignosis eFront LMS 代码问题漏洞（CNNVD-201909-056） |
| | | CNNVD-201909-048 | 联想 | |
| | | CNNVD-201909-818 | Schneider Electric | |
| | | CNNVD-201909-820 | | |
| | | CNNVD-201909-839 | | |

| | | | | |
|---|---|---|---|---|
| | | CNNVD-201909-154 | Qualcomm | |
| | | CNNVD-201909-177 | | |
| | | CNNVD-201909-712 | Pimcore | |
| | | CNNVD-201909-809 | Micro Focus | |
| | | CNNVD-201909-566 | Linux | |
| | | CNNVD-201909-567 | | |
| | | CNNVD-201909-568 | | |
| | | CNNVD-201909-570 | | |
| | | CNNVD-201909-571 | | |
| | | CNNVD-201909-572 | | |
| | | CNNVD-201909-1164 | HCL Technologies | |
| | | CNNVD-201909-008 | GitLab | |
| | | CNNVD-201909-010 | | |
| | | CNNVD-201909-361 | | |
| | | CNNVD-201909-056 | Epignosis | |
| | | CNNVD-201909-1114 | Cisco | |
| | | CNNVD-201909-1122 | | |
| | | CNNVD-201909-159 | | |
| | | CNNVD-201909-444 | Adobe | |
| 15 | 操作系统命令注入 | CNNVD-201909-632 | CloudBees | CloudBees Jenkins Git Client Plugin 操作系统命令注入漏洞（CNNVD-201909-632） |
| | | CNNVD-201909-834 | 研华 | |
| 16 | SQL 注入 | CNNVD-201909-023 | Panasonic | Panasonic Video Insight VMS SQL 注入漏洞（CNNVD-201909-023） |
| | | CNNVD-201909-1084 | Progress Software | |
| | | CNNVD-201909-587 | Dell | |

## 1. IBM Cognos Analytics 资源管理错误漏洞（CNNVD-201909-724）

IBM Cognos Analytics 是美国 IBM 公司的一套商业智能软件。该软件包括报表、仪表板和记分卡等，并可通过分析关键因素与关键人等内容，协助企业调整决策。

IBM Cognos Analytics 11.1 版本和 11.0 版本中存在资源管理错误漏洞。远程攻击者可借助特制的请求利用该漏洞消耗所有可用资源，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://www.ibm.com/support/pages/node/1073530

2. Cisco Webex Teams 注入漏洞（CNNVD-201909-160）

Cisco Webex Teams 是美国思科（Cisco）公司的一款团队协作应用程序。该程序包括视频会议、消息群发和文件共享功能。

基于 Windows 平台的 Cisco Webex Teams 3.0.12427.0 之前版本中存在注入漏洞，该漏洞源于程序没有正确限制软件日志记录功能。远程攻击者可通过诱使用户访问网站并通过该网站发送恶意的输入利用该漏洞修改文件并在系统上以目标用户权限在系统上执行任意命令。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190904-webex-teams

3. Bosch Access Professional Edition 信息泄露漏洞（CNNVD-201909-651）

Bosch Access Professional Edition 是德国博世（Bosch）公司的一

套企业访问控制和安防管理解决方案。该产品支持视频监控、实时报警等功能。

Bosch Access Professional Edition 3.7 及之前版本中存在信息泄露漏洞。攻击者可利用该漏洞获取敏感数据的访问权限。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://psirt.bosch.com/Advisory/BOSCH-SA-844044.html

4. Dell EMC Enterprise Copy Data Management 信任管理问题漏洞（CNNVD-201909-043）

Dell EMC Enterprise Copy Data Management（eCDM）是美国戴尔（Dell）公司的一套企业副本数据管理解决方案。

Dell EMC eCDM 中存在信任管理问题漏洞。远程攻击者可通过提交特制的证书并拦截用户流量利用该漏洞实施中间人攻击。以下产品及版本受到影响：

- Dell EMC eCDM 1.0 版本
- Dell EMC eCDM 1.1 版本
- Dell EMC eCDM 2.0 版本
- Dell EMC eCDM 2.1 版本
- Dell EMC eCDM 3.0 版本

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.dell.com/support/security/zh-cn/details/536848/DSA-2019-118-Dell-EMC-Enterprise-Copy-Data-Management-eCDM-Improper-Certificate-Validation-Vuln

5. Cisco IOS XE 输入验证错误漏洞（CNNVD-201909-1162）

Cisco IOS XE 是美国思科（Cisco）公司的一套为其网络设备开发的操作系统。

Cisco IOS XE 中的 Unified Threat Defense (UTD)存在输入验证错误漏洞，该漏洞源于 UTD 功能没有正确验证 IPv6 数据包。远程攻击者可通过发送 IPv6 流量利用该漏洞造成拒绝服务。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-utd

6. GitLab 授权问题漏洞（CNNVD-201909-339）

GitLab 是美国 GitLab 公司的一款使用 Ruby on Rails 开发的、自托管的、Git（版本控制系统）项目仓库应用程序。该程序可用于查阅项目的文件内容、提交历史、Bug 列表等。

GitLab 中存在授权问题漏洞。攻击者可利用该漏洞绕过邮件验证。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://about.gitlab.com/2019/07/29/security-release-gitlab-12-dot-1-dot-2-released/

7. Android NVIDIA BootROM 权限许可和访问控制问题漏洞（CNNVD-201909-176）

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。NVIDIA BootROM 是其中的一个 Boot ROM 组件。

Android 中的 NVIDIA BootROM 组件存在权限许可和访问控制问题漏洞。攻击者可利用该漏洞向任意的物理地址写入任意值。

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/2019-09-01

8. Cisco IOS XE 命令注入漏洞（CNNVD-201909-1139）

Cisco IOS XE 是美国思科（Cisco）公司的一套为其网络设备开发的操作系统。

Cisco IOS XE 中基于 Web 的用户界面存在命令注入漏洞，该漏洞源于程序没有正确处理用户提交的输入。攻击者可借助特制的输入参数利用该漏洞以提升的权限（15 级）执行 Cisco IOS 命令。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-webui-cmd-injection

9. 3S-Smart Software Solutions CODESYS V3 web server 路径遍历漏洞（CNNVD-201909-657）

3S-Smart Software Solutions CODESYS V3 web server 是德国 3S-Smart Software Solutions 公司的一款使用在 CODESYS 产品中的 Web 服务器。

3S-Smart Software Solutions CODESYS V3 web server 3.5.14.10 之前版本中存在路径遍历漏洞。攻击者可通过发送特制的 http 或 https 请求利用该漏洞访问被限制工作目录之外的文件。

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.codesys.com/

10. Dell EMC Integrated Data Protection Appliance 跨站脚本漏洞（CNNVD-201909-1310）

Dell EMC Integrated Data Protection Appliance 是美国戴尔（Dell）公司的一套基于磁盘的备份和恢复解决方案。

Dell EMC Integrated Data Protection Appliance 2.3 之前版本中存在跨站脚本漏洞。远程攻击者可利用该漏洞执行恶意代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.dell.com/support/security/zh-cn/details/536363/DSA-2019-112-Dell-EMC-Integrated-Data-Protection-Appliance-Multiple-Vulnerabilities

11. Mozilla Firefox 竞争条件问题漏洞（CNNVD-201909-049）

Mozilla Firefox 是美国 Mozilla 基金会的一款开源 Web 浏览器。

基于 Windows 平台的 Mozilla Firefox 69 之前版本中存在竞争条件问题漏洞。攻击者可利用该漏洞获取提升的权限。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.mozilla.org/en-US/security/advisories/mfsa2019-25/

12. Microsoft Internet Explorer 缓冲区错误漏洞（CNNVD-201909-1071）

Microsoft Internet Explorer（IE）是美国微软（Microsoft）公司的一款 Windows 操作系统附带的 Web 浏览器。

Microsoft IE 9、10 和 11 中脚本引擎处理内存对象的方法存在缓冲

区错误漏洞。攻击者可利用该漏洞在当前用户的上下文中执行任意代码，造成内存损坏。

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-2019-1367

13. Dell RSA Identity Governance and Lifecycle 和 RSA Via Lifecycle and Governance 代码注入漏洞（CNNVD-201909-585）

Dell RSA Identity Governance and Lifecycle 和 RSA Via Lifecycle and Governance 都是美国戴尔（Dell）公司的一套身份验证和生命周期管理解决方案。

Dell RSA Identity Governance and Lifecycle 和 RSA Via Lifecycle and Governance 7.1.0 P08 之前版本中存在代码注入漏洞。远程攻击者可利用该漏洞获取有限的权限，进而查看或修改 Workflow 系统上的信息。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.dell.com/support/security/zh-cn/details/DOC-106943/DSA-2019-134-RSA-Identity-Governance-and-Lifecycle-Product-Security-Update-for-Multiple-Vulnerabi

14. Epignosis eFront LMS 代码问题漏洞（CNNVD-201909-056）

Epignosis eFront LMS 是美国 Epignosis 公司的一套在线电子学习平台。该平台提供测试构建、作业管理、内部消息传递、论坛和在线聊天等功能。

Epignosis eFront LMS 5.2.12 版本中存在代码问题漏洞。攻击者可借助特制的 Web 请求利用该漏洞执行 PHP 代码。

目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：

https://www.efrontlearning.com/

15. CloudBees Jenkins Git Client Plugin 操作系统命令注入漏洞（CNNVD-201909-632）

CloudBees Jenkins（Hudson Labs）是美国 CloudBees 公司的一套基于 Java 开发的持续集成工具。该产品主要用于监控持续的软件版本发布/测试项目和一些定时执行的任务。Git Client Plugin 是使用在其中的一个 Git 客户端插件。

CloudBees Jenkins Git Client Plugin 2.8.4 及之前版本中存在操作系统命令注入漏洞。攻击者可利用该漏洞执行操作系统命令。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://jenkins.io/security/advisory/2019-09-12/

16. Panasonic Video Insight VMS SQL 注入漏洞（CNNVD-201909-023）

Panasonic Video Insight VMS 是日本松下电器（Panasonic）公司的一套企业监控视频管理系统。

Panasonic Video Insight VMS 7.3.2.5 及之前版本中存在 SQL 注入漏洞。远程攻击者可利用该漏洞对数据库执行任意的 SQL 语句。

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.panasonic.com/global/home.html

## 二、接报漏洞情况

本月接报漏洞共计 6784 个，其中信息技术产品漏洞（通用型漏洞）75 个，网络信息系统漏洞（事件型漏洞）6709 个。

表 7 2018 年 9 月漏洞接报情况

| 序号 | 报送单位 | 漏洞总量 | 通用型漏洞 | 事件型漏洞 |
|---|---|---|---|---|
| 1 | 上海斗象信息科技有限公司 | 3335 | 0 | 3335 |
| 2 | 网神信息技术（北京）股份有限公司 | 3152 | 0 | 3152 |
| 3 | 山东新潮信息技术有限公司 | 76 | 0 | 76 |
| 4 | 北京数字观星科技有限公司 | 50 | 0 | 50 |
| 5 | 北京智游网安科技有限公司 | 30 | 30 | 0 |
| 6 | 广州锦行网络科技有限公司 | 21 | 1 | 20 |
| 7 | 中新网络信息安全股份有限公司 | 19 | 0 | 19 |
| 8 | 北京天融信网络安全技术有限公司 | 12 | 0 | 12 |
| 9 | 内蒙古奥创科技有限公司 | 11 | 0 | 11 |
| 10 | 国发中新（北京）科技发展有限公司 | 10 | 0 | 10 |
| 11 | 北京神州绿盟科技有限公司安全研究部 | 9 | 9 | 0 |
| 12 | 北京圣博润高新技术股份有限公司 | 9 | 1 | 8 |
| 13 | 中兴通讯 | 8 | 8 | 0 |
| 14 | 上海安识网络科技有限公司 | 6 | 0 | 6 |
| 15 | 广州竞远安全技术股份有限公司 | 5 | 1 | 4 |
| 16 | 四川虹微技术有限公司 | 4 | 4 | 0 |
| 17 | 苏州极光无限信息技术有限公司 | 3 | 3 | 0 |

| | | | | |
|---|---|---|---|---|
| **18** | 北京威努特技术有限公司 | 3 | 3 | 0 |
| **19** | 西安交大捷普网络科技有限公司 | 3 | 0 | 3 |
| **20** | 北京中金安服科技有限公司 | 3 | 0 | 3 |
| **21** | 个人 | 3 | 3 | 0 |
| **22** | 东软集团股份有限公司 | 2 | 2 | 0 |
| **23** | 广州万方计算机科技有限公司 | 2 | 2 | 0 |
| **24** | 西安四叶草信息技术有限公司 | 2 | 2 | 0 |
| **25** | 北京山石网科信息技术有限公司 | 1 | 1 | 0 |
| **26** | 绿盟科技 | 1 | 1 | 0 |
| **27** | 北京安信天行科技有限公司 | 1 | 1 | 0 |
| **28** | 亚信科技（成都）有限公司 | 1 | 1 | 0 |
| **29** | 山东正中信息技术股份有限公司-检测部 | 1 | 1 | 0 |
| **30** | 北京邮电大学 | 1 | 1 | 0 |
| 报送总计 | | 6784 | 75 | 6709 |

# 三、重大漏洞预警

## 3.1 关于 Internet Explorer 远程代码执行漏洞的通报

本月，国家信息安全漏洞库（CNNVD）收到关于 Internet Explorer 远程代码执行漏洞（CNNVD-201909-1071、CVE-2019-1367）情况的报送。成功利用此漏洞的攻击者，可以获得当前用户的所有权限，并执行任意代码。InternetExplorer 9、10、11 等多个版本均受此漏洞影响。目前，微软官方已经发布更新修复了该漏洞，请用户及时确认是否受到漏洞影响，尽快采取修补措施。

### 漏洞简介

Internet Explorer 是微软公司推出的一款浏览器。2019 年 9 月 23 日微软紧急发布安全更新，修复了一个影响 IE 浏览器的远程代码执行漏洞。微软指出，该漏洞能够损坏内存，使攻击者能够在当前用户的上下文中执行任意代码。成功利用该漏洞的攻击者能够获取和当前用户一样的用户权限。如当前用户以管理员权限登录，攻击者便能够控制受影响系统，随后执行安装程序、查看、更改、删除数据、或者创建管理员账户。

### 漏洞危害

成功利用此漏洞的攻击者，可以获得当前用户的所有权限，并执行任意代码。InternetExplorer 9、10、11 等多个版本均受此漏洞影响

**修复措施**

目前，微软官方已经发布更新修复了该漏洞，请用户及时确认是否受到漏洞影响，尽快采取修补措施。微软官方更新链接地址：

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1367

## 3.2 关于 IBM WebSphere 任意文件读取漏洞情况的通报

本月，国家信息安全漏洞库（CNNVD）收到关于 IBM WebSphere 任意文件读取漏洞（CNNVD-201909-864、CVE-2019-4505）情况的报送。成功利用此漏洞的攻击者，可以读取目标系统特定目录下的任意文件，造成 IBM WebSphere 账号及数据库配置等敏感信息泄漏。WebSphere Application Server Version 7.0、8.0、8.5、9.0 等多个版本均受此漏洞影响。目前，IBM 官方已经发布更新修复了该漏洞，请用户及时确认是否受到漏洞影响，尽快采取修补措施。

漏洞简介

IBM WebSphere Application Server 是美国 IBM 公司的一款应用服务器产品。该产品是 JavaEE 和 Web 服务应用程序的平台，也是 IBMWebSphere 软件平台的基础。该漏洞存在于 MiddlewareAgentWebapp.war 文件中，攻击者可以攻击者可对远程目标系统的/MiddlewareAgentRPCService/noadmin/发出 GET 请求，以此读取目标系统特定目录下的任意文件，获取登陆控制台用户 id 及密码 hash，造成 Websphere 账号及数据库配置等敏感信息泄漏。

通过对 IBM WebSphere 在互联网中的 IP 地址进行分析，2019 年全球共 35911 个用户，国内共 10080 个，其中域名为 gov 的政府用户共 50 个。目前该漏洞 poc 已经在网络中流传，存在较大风险，建议用户及时修复。

## 漏洞危害

成功利用此漏洞的攻击者，可以读取目标系统特定目录下的任意文件，造成 IBM WebSphere 账号及数据库配置等敏感信息泄漏。受漏洞影响版本如下：

WebSphere Application Server Version 9.0

WebSphere Application Server Version 8.5

WebSphere Application Server Version 8.0

WebSphere Application Server Version7.0

## 安全建议

目前，IBM 官方已经发布更新修复了该漏洞，请用户及时确认是否受到漏洞影响，尽快采取修补措施。IBM 官方更新链接地址：

https://www.ibm.com/support/pages/node/964766