北京师范大学网络信息安全通告

2019 年 2 月报告

北京师范大学信息网络中心

2019 年 3 月

目录

漏洞态势

根据国家信息安全漏洞库（CNNVD）统计，2019 年 2 月份采集安全漏洞共 1038 个。本月接报漏洞共计 2720 个，其中信息技术产品漏洞（通用型漏洞）32 个，网络信息系统漏洞（事件型漏洞）2688 个。

重大漏洞预警

1 、 WinRAR 存在代码执行漏洞 （CNNVD-201902-077、CVE-2018-20250）：攻击者利用该漏洞可以进行远程代码执行攻击。目前，WinRAR 官方已经发布更新修复了该漏洞。

2、微软多个安全漏洞：微软官方发布了多个安全漏洞的公告，包括 Microsoft Office 安全功能绕过漏洞（CNNVD-201902-356、CVE-2019-0540 ）、Windows 脚本引擎内存损坏漏洞（CNNVD-201902-405、CVE-2019-0590）、Microsoft SharePoint 远程代码执行漏洞（CNNVD-201902-349、CVE-2019-0594）等。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。

1. 公开漏洞情况

根据国家信息安全漏洞库（CNNVD）统计，2019 年 2 月份新增安全漏洞共 1038 个，从厂商分布来看，Microsoft 公司产品的漏洞数量最多，共发布 77 个；从漏洞类型来看，跨站脚本类的漏洞占比最大，达到 14.45%。本月新增漏洞中，超危漏洞 109 个、高危漏洞 239 个、中危漏洞 608 个、低危漏洞 10 个，相应修复率分别为 63.30%、59.83%、87.17%以及 80.00%。合计 750 个漏洞已有修复补丁发布，本月整体修复率 72.25%。截至 2019 年 2 月 28 日，CNNVD 采集漏洞总量已达 122396 个。

1.1. 漏洞增长概况

2019 年 2 月新增安全漏洞 1038 个，与上月（1463 个）相比减少了 29.05%。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 1265 个。

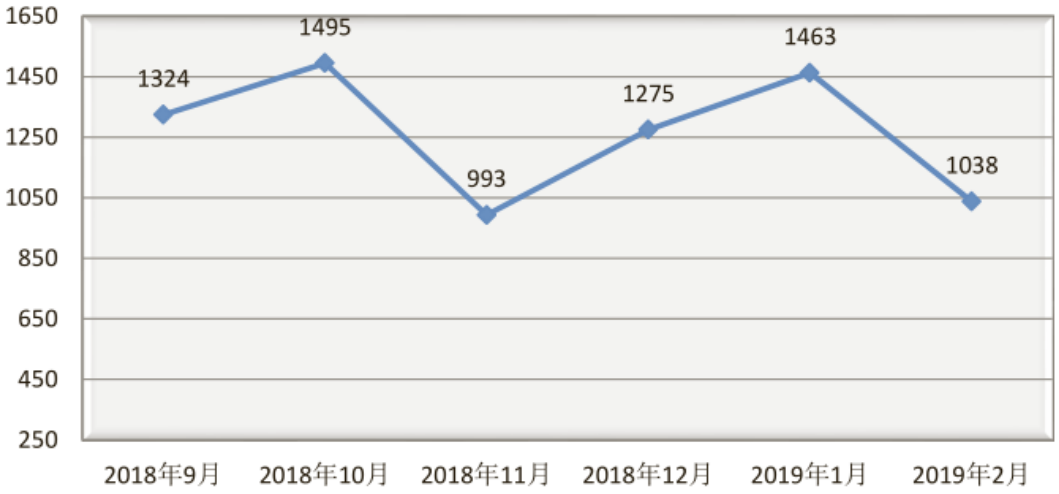

图 1 2018 年 9 月至 2019 年 2 月漏洞新增数量统计图

1.2. 漏洞分布情况

1.2.1. 漏洞厂商分布

2 月厂商漏洞数量分布情况如表 1 所示，微软公司达到 77 个，占本月漏洞总量的 7.42%。本月 Adobe、Cisco、Google 等公司的漏洞数量均有所上升，Intel、SAP 等厂商的漏洞数量出现较不同程度的下降。

表1 2019 年 2 月新增安全漏洞排名前十厂商统计表

序号	厂商名称	漏洞数量	所占比例
1	微软	77	7.42%
2	Adobe	74	7.13%
3	谷歌	34	3.28%
4	CloudBees	30	2.89%
5	思科	28	2.89%
6	IBM	25	2.70%
7	友讯	20	2.41%
8	Intel	14	1.93%
9	SAP	12	1.35%
10	Qualcomm	11	1.06%

1.2.2. 漏洞产品分布

2 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 31 条，其中桌面操作系统 31 条，服务器操作系统 31 条。本月 Microsoft Windows 10 和 Microsoft Windows Server1709 漏洞数量最多，各 29 个，占主流操作系统漏洞总量的 25.89%，排名第一。

表 2 2019 年 2 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	Microsoft Windows 10	29

2	Microsoft Windows Server 1709	29
3	Microsoft Windows Server 2016	28
4	Microsoft Windows Server 2012	26
5	Microsoft Windows 8.1	25
6	Microsoft Windows Rt 8.1	24
7	Microsoft Windows 7	24
8	Microsoft Windows Server 2008	24
9	Linux Kernel	8
10	Android	4
11	Apple iOS	3

说明：

* 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

2 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 14.45%。

表3　2019 年 2 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	150	14.45%
2	缓冲区错误	133	12.81%

3	输入验证	65	6.26%
4	信息泄露	44	4.24%
5	路径遍历	36	3.47%
6	跨站请求伪造	32	3.08%
7	SQL 注入	27	2.60%
8	访问控制错误	23	2.22%
9	权限许可和访问控制	23	2.22%
10	命令注入	22	2.12%
11	代码注入	15	1.45%
12	资源管理错误	14	1.35%
13	信任管理	13	1.25%
14	注入	10	0.96%
15	授权问题	9	0.87%
16	安全特征问题	7	0.67%
17	数字错误	7	0.67%
18	操作系统命令注入	6	0.58%
19	竞争条件	4	0.39%
20	加密问题	2	0.19%
21	格式化字符串	1	0.10%
22	后置链接	1	0.10%

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。2 月漏洞危害等级分布如图 2 所示，其中超危漏洞 109 条，占本月漏洞总数的 10.50%。

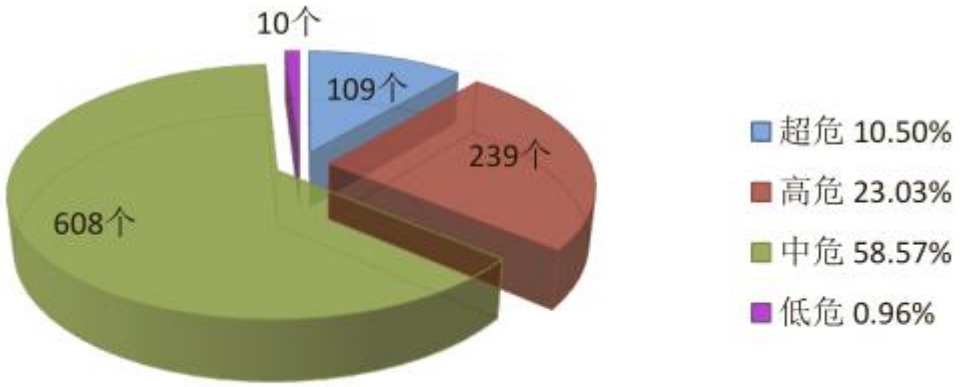

图 2　2019 年 2 月漏洞危害等级分布

1.3. 漏洞修复情况

1.3.1. 整体修复情况

2 月漏洞修复情况按危害等级进行统计见图 3。其中中危漏洞修复率最高，达到 87.17%，高危漏洞修复率最低，比例为 59.83%。与上月相比，本月中危、低危漏洞修复率有所上升，高危、超危漏洞修复率有所下降。总体来看，本月整体修复率上升，由上月的 59.06%上升至本月的 72.25%。

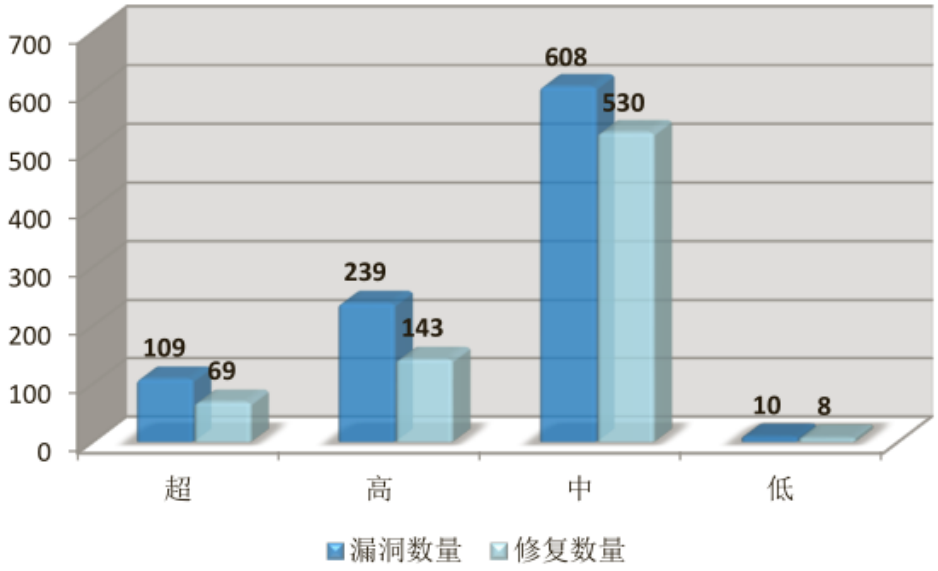

图 3　2019 年 2 月漏洞修复数量统计

1.3.2. 厂商修复情况

2 月漏洞修复情况按漏洞数量前十厂商进行统计，其中思科、谷歌、微软等十个厂商共 325 条漏洞，占本月漏洞总数的 31.31%，漏洞修复率为 92.00%，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 Adobe、谷歌、Mozilla、Intel、SAP 等公司本月漏洞修复率均为 100%，共 256 条漏洞已全部修复。

表 4 2019 年 2 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	微软	77	76	98.70%
2	Adobe	74	74	100.00%
3	谷歌	34	34	100.00%
4	CloudBees	30	28	93.33%
5	思科	28	21	75.00%
6	IBM	25	22	88.00%
7	友讯	20	7	35.00%
8	Intel	14	14	100.00%
9	SAP	12	12	100.00%
10	Qualcomm	11	11	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 109 个，其中重要漏洞实例如表 5 所示。

表 5 2019 年 2 月超危漏洞实例

序号	漏洞类型	CNNVD 编号	厂商	漏洞实例
1	安全特征问题	CNNVD-201902-647	ZOHO	ZOHO ManageEngine ServiceDesk Plus 安全特征问题漏洞

2	访问控制错误	CNNVD-201901-972	Yokogawa	多款Yokogawa产品访问控制错误漏洞
3	缓冲区错误	CNNVD-201901-1010	Mozilla	Mozilla Firefox 和 Firefox ESR 缓冲区错误漏洞
		CNNVD-201902-907	Flexera Software	
4	权限许可和访问控制	CNNVD-201901-1007	Mozilla	SolarWinds Orion Network Performance Monitor权限许可和访问控制漏洞
		CNNVD-201901-1054	SchedMD	
		CNNVD-201902-702	Intel	
		CNNVD-201902-717	SolarWinds	
5	输入验证	CNNVD-201902-548	D-circle	ThinkPHP 输入验证漏洞
		CNNVD-201902-884	顶想信息科技	

1. **ZOHO ManageEngine ServiceDesk Plus 安全特征问题漏洞（CNNVD-201902-647）**

ZOHO ManageEngine ServiceDesk Plus（SDP）是美国卓豪（ZOHO）公司的一套基于 ITIL 架构的 IT 服务管理软件。该软件集成了事件管理、问题管理、资产管理 IT 项目管理、采购与合同管理等功能模块。ZOHO ManageEngine SDP 10.0 build 10007 之前版本中存在安全特征问题漏洞。远程攻击者可通过发送特制的请求利用该漏洞获取敏感信息。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：
https://www.manageengine.com/products/service-desk/readme.html

2. **多款 a Yokogawa 产品访问控制错误漏洞（CNNVD- 201901-972）**

Yokogawa CENTUM VP 等都是都是日本横河电机（Yokogawa）公司的产品。Yokogawa CENTUM VP 是一套综合生产控制系统。ProSafe-RS 是一套安全仪表系统。License Manager Service 是使用在其中的一个许可证管理服务。多款

Yokogawa 产品中存在安全漏洞，该漏洞源于程序没有正确地限制恶意文件的上传。攻击者可利用该漏洞执行任意代码。以下产品受和版本受到影响：

- Yokogawa CENTUM VP R5.01.00 版本至 R6.06.00 版本
- Yokogawa CENTUM VP Entry Class R5.01.00 版本至 R6.06.00 版本
- Yokogawa ProSafe-RS R3.01.00 版本至 R4.04.00 版本
- Yokogawa PRM R4.01.00 版本至 R4.02.00 版本
- Yokogawa B/M9000 VP R7.01.01 版本至 R8.02.03 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：http://www.yokogawa.com

3. Mozilla Firefox 和 Firefox ESR 缓冲区错误漏洞（CNNVD-201901-1010）

Mozilla Firefox 和 Firefox ESR 都是美国 Mozilla 基金会开发的浏览器产品。Firefox 是一款开源 Web 浏览器；Firefox ESR 是 Firefox 的一个延长支持版本。Mozilla Firefox 64 版本和 Firefox ESR 60.4 版本中存在缓冲区错误漏洞。攻击者可利用该漏洞损坏内存并可能执行任意代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.mozilla.org/en-US/security/advisories/mfsa2019-01/

4. SolarWinds Orion Network Performance Monitor 权限许可和访问控制漏洞（CNNVD-201902-717）

SolarWinds Orion Network Performance Monitor（NPM）是美国 SolarWinds 公司的一款网络性能监视器。该产品为路由器、虚拟化环境和其他设备提供监控和报告、跟踪 up/down 状态、实时分析和网络性能统计等功能。SolarWinds Orion NPM 12.4 之前版本中的 OrionModuleEngine 服务存在权限许可和访问控制漏洞。攻击者可借助 InvokeActionMethod 方法利用该漏洞以 SYSTEM 用户身份执行命令。

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.solarwinds.com/

5. ThinkP HP 输入验证漏洞（CNNVD-201902-884）

ThinkPHP 是中国顶想信息科技公司的一套基于 PHP 的、开源的、轻量级 Web 应用程序开发框架。ThinkPHP 3.2.4 之前版本中（使用在 Open Source BMS v1.1.1 版本和其他设备上）中存在输入验证漏洞。远程攻击者可借助 public//?s=index/hinkapp/invokefunction&function=call_user_func_array &vars[0]=system&vars[1][]= URL 利用该漏洞执行命令。

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：http://www.thinkphp.cn/

1.4.2. 高危漏洞实例

本月高危漏洞共 239 个，其中重点漏洞实例如表 6 所示。

表 6 2019 年 2 月高危漏洞实例

序号	漏洞类型	CNNVD 编号	厂商	漏洞实例
1	安全特征问题	CNNVD-201901-963	PowerDNS	PowerDNS Recursor 安全特征问题漏洞
		CNNVD-201902-776	CloudBees	
2	操作系统命令注入	CNNVD-201902-773	Cisco	Cisco HyperFlex Software 操作系统命令注入漏洞
3	代码注入	CNNVD-201902-755	WordPress	WordPress 代码注入漏洞
4	访问控制错误	CNNVD-201902-605	Amazon	SAP HANA Extended Application Services 访问控制错误漏洞
		CNNVD-201902-793	Cisco	
		CNNVD-201902-786	Micro Focus	
		CNNVD-201902-519	SAP	

5	后置链接	CNNVD-201902-699	LG	LG Device Manager LHA.sys 驱动程序后置链接漏洞
6	缓冲区错误	CNNVD-201901-1034 CNNVD-201901-1032	ACD Systems	ACD Systems Canvas Draw 缓冲区错误漏洞
		CNNVD-201902-467	Adobe	
		CNNVD-201901-984 CNNVD-201901-993 CNNVD-201901-992	Google	
		CNNVD-201902-924 CNNVD-201902-331	Qualcomm	
7	权限许可和访问控制	CNNVD-201902-316	Docker	Intel Data Center Manager SDK 权限许可和访问控制漏洞
		CNNVD-201902-708 CNNVD-201902-694	Intel	
8	输入验证	CNNVD-201902-295 CNNVD-201902-802	Cisco	Google Chrome DevTools 输入验证漏洞
		CNNVD-201902-749 CNNVD-201901-1002 CNNVD-201901-991 CNNVD-201901-996 CNNVD-201901-985 CNNVD-201901-976	Google	
		CNNVD-201902-537	Siemens	
9	信息泄露	CNNVD-201901-1027	Apache	CloudBees Jenkins Cloud Foundry Plugin 信息泄露漏洞
		CNNVD-201902-778	CloudBees	

1. PowerDNS Recursor 安全特征问题漏洞（CNNVD-201901-963）

PowerDNS Recursor（又名 pdns_recursor）是荷兰 PowerDNS 公司的一款域名解析服务器。PowerDNS Recursor 4.1.4 版本至 4.1.8 版本中存在安全特征问题漏洞，该漏洞源于程序没有对通过 TCP 协议所接收到的查询执行 Luahooks 机制。远程攻击者可利用该漏洞绕过安全策略。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://docs.powerdns.com/recursor/security-advisories/powerdns-advisory-2019-01.html

2. Cisco HyperFlex Software 操作系统命令注入漏洞（CNNVD-201902-773）

Cisco HyperFlex Software 是美国思科（Cisco）公司的一套套可扩展的分布式文件系统。该系统通过云管理提供统一的计算、存储和网络，并提供企业级数据管理和优化服务。Cisco HyperFlex Software 3.5(2a)之前版本中的 cluster servicemanager 存在操作系统命令注入漏洞，该漏洞源于不充分的输入验证。攻击者可通过连接到集群服务管理器并注入命令利用该漏洞以 root 用户身份执行命令。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvj95590。

3. WordPress 代码注入漏洞（CNNVD-201902-755）

WordPress 是 WordPress 基金会的一套使用 PHP 语言开发的博客平台。该平台支持在 PHP 和 MySQL 的服务器上架设个人博客网站。WordPress 4.9.9 之前版本和 5.0.1 之前的 5.x 版本中存在代码注入漏洞。远程攻击者可通过上传包含有 PHP 代码的特制图像利用该漏洞执行任意代码。

目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：http://www.wordpress.org/

4. SAP HANA Extended Application Services 访问控制错误漏洞（CNNVD-201902-519）

SAP HANA 是德国思爱普（SAP）公司的一套高性能的实时数据分析平台。该平台提供数据查询功能，支持用户对查询实时业务数据进行查询和分析。Extended Application Services 是一个应用程序服务器、Web 服务器和 SAP

HANA System 内 Web 应用的开发环境。SAP HANA Extended Application Services 中存在访问控制错误漏洞。远程攻击者可利用该漏洞获取敏感信息。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=510922950

5. LG Device Manager s LHA.sys 驱动程序后置链接漏洞（CNNVD-201902-699）

LG Device Manager 是韩国乐金（LG）公司的一款设备管理器。LHA.sys driver 是其中的一个 LHA.sys 驱动程序。LG Device Manager 中的 LHA.sys 驱动程序 1.1.1811.2101 之前版本存在后置链接漏洞，该漏洞源于设备对象带有与之相关联的符号链接和开放的 DACL。攻击者可借助特制的 IOCTL 请求利用该漏洞读取并写入任意的物理内存。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://lgsecurity.lge.com/security_updates.html

6. ACD Systems Canvas Draw 缓冲区错误漏洞（CNNVD-201901-1034）

ACD Systems Canvas Draw 是美国 ACD Systems 公司的一款图形编辑工具，它主要用于创建和编辑图像等。ACD Systems Canvas Draw 5.0.0.28 版本中的 CALS Raster 文件解析功能存在越界写入漏洞。攻击者可借助特制的 CAL 图像利用该漏洞覆盖任意数据，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.acdsystems.com/

7. Intel Data Center Manager SDK 权限许可和访问控制漏洞（CNNVD-201902-694）

Intel Data Center Manager SDK 是美国英特尔（Intel）公司的一款数据中心管理 SDK（软件开发工具包）。该产品主要提供设备实时电源和散热数

据。Intel(R) Data Center Manager SDK 5.0.2 之前版本中的安装例行进程存在权限许可和访问控制漏洞，该漏洞源于程序没有对文件权限进行充分的检查。本地攻击者可利用该漏洞提升权限。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：
https://www.intel.com/content/www/us/en/security-center/advisory/INTEL-SA-00215.html

8. Google Chrome DevTools 输入验证漏洞（CNNVD-201902-749）

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。Devtools 是其中的一个开发调试工具。Google Chrome 72.0.3626.81 之前版本中的 DevTools 存在输入验证漏洞，该漏洞源于程序未充分地验证不可信的输入。攻击者可借助特制的 HTML 页面利用该漏洞泄露信息。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：
https://chromereleases.googleblog.com/2019/01/stable-channel-update-for-desktop.html

9. CloudBees Jenkins Cloud Foundry Plugin 信息泄露漏洞（CNNVD-201902-778）

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。Cloud Foundry Plugin 是使用在其中的一个用于将项目推送到 Cloud Foundry 平台的插件。CloudBees Jenkins Cloud Foundry Plugin 2.3.1 及之前版本中的 AbstractCloudFoundryPushDescriptor.java 文件存在信息泄露漏洞。攻击者可利用该漏洞捕获存储在 Jenkins 中的凭证。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：
https://jenkins.io/security/advisory/2019-02-19/#SECURITY-876

2. 接报漏洞情况

本月接报漏洞共计 2720 个，其中信息技术产品漏洞（通用型漏洞）32 个，网络信息系统漏洞（事件型漏洞）2688 个

表 7　2019 年 2 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	1320	0	1320
2	网神信息技术（北京）股份有限公司	903	0	903
3	中新网络信息安全股份有限公司	217	3	214
4	河南听潮盛世信息技术有限公司	113	2	111
5	北京数字观星科技有限公司	66	0	66
6	新华三技术有限公司	27	0	27
7	国发中新（北京）科技发展有限公司	15	0	15
8	北京天地和兴科技有限公司	14	0	14
9	西安交大捷普网络科技有限公司	7	5	2
10	北京圣溥润高新技术服份有限公司	6	0	6
11	杭州迪普科技股份有限公司	6	0	6
12	内蒙古奥创科技有限公司	5	1	4
13	长亭科技（ChaitinTech）	4	4	0
14	北京启明星辰信息安全技术有限公司	4	4	0
15	杭州安恒信息技术股份有限公司	3	3	0
16	山东华鲁科技发展股份有限公司	2	2	0

17	厦门服云信息科技有限公司	2	2	0
18	山东维平信息安全测评技术有限公司	2	2	0
19	腾讯安全云鼎实验室	1	1	0
20	哈尔滨安天科技集团股份有限公司	1	1	0
21	河北华测信息技术有限公司	1	1	0
22	北京壹号车科技有限公司	1	1	0
报送总计		2720	32	2688

3. 重大漏洞预警

3.1. 关于 ThinkPHP5.0 远程代码执行漏洞(CNNVD-201901-445)的通报

近日，国家信息安全漏洞库（CNNVD）收到关于 WinRAR 代码执行漏洞（CNNVD-201902-077、CVE-2018-20250）情况的报送。攻击者利用该漏洞可以进行代码执行攻击。WinRAR 5.70 Beta 1 以下版本均受上述漏洞影响。目前，部分漏洞的验证工具已经公开，此外 WinRAR 官方已经发布更新修复了该漏洞，建议受该漏洞影响的 WinRAR 用户尽快采取修补措施。

漏洞简介

WinRAR 是 Windows 平台上最为知名的解压缩软件，它能解压缩 RAR、ZIP、7z、ACE 等多种压缩格式的软件。目前该软件官网称其在全球有超过 5 亿用户。该漏洞形成原因是 WinRAR 在解压处理 ACE 格式的文件过程中，未对 ACE 文件头结构中的“filename”字段进行充分过滤，导致路径穿越漏洞。攻击者利用该漏洞可以向受害者计算机开机启动目录中写入恶意文件，导致计算机重启时执行恶意代码。

漏洞危害

攻击者利用 WinRAR 该漏洞可以进行远程代码执行攻击。目前，该漏洞验证工具已经公开。近期，利用该漏洞进行网络攻击的可能性较高。受漏洞影响版本如下：

WinRAR 5.70 Beta 1 以下版本

修复措施目前，WinRAR 官方已经发布更新修复了上述漏洞，请用户及时检查产品版本，如确认受到漏洞影响，可按以下措施进行防护。

（1）升级 WinRAR 版本：Windows 系统下升级至最新的 5.70 Beta 1 版本：https://www.rarlab.com/download.htm

（2）若用户无法立即升级版本，临时缓解方案：删除老版本 WinRAR 安装目录中 unacev2.dll 文件

3.2. 关于微软多个安全漏洞的通报

近日，微软官方发布了多个安全漏洞的公告，包括 MicrosoftOffice 安全功能绕过漏洞（CNNVD-201902-356、CVE-2019-0540）、Windows 脚本引擎内存损坏漏洞（CNNVD-201902-405、CVE-2019-0590）、Microsoft SharePoint 远程执行代码漏洞（CNNVD-201902-349、CVE-2019-0594）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。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，采取修补措施。

漏洞简介

本次漏洞公告涉及 Microsoft Windows 系统、Microsoft Office、Microsoft SharePoint、Microsoft Edge、Internet Explorer、WindowsDHCP 客户端等 Windows 平台下应用软件和组件。漏洞详情如下：

1、Microsoft Office 安全功能绕过漏洞（CNNVD-201902-356、CVE-2019-0540）

漏洞简介：当 Microsoft Office 不验证 URL 时，存在安全功能绕过漏洞。攻击者通过设计一个特殊构造的文件诱使用户将其打开，从而获取用户计算机中存储的数据。

2、Windows 脚本引擎内存损坏漏洞（CNNVD-201902-405、CVE-2019-0590）、（CNNVD-201902-513、CVE-2019-0591）、（CNNVD-201902-406、CVE-2019-0593）、（CNNVD-201902-385、CVE-2019-0640）

漏洞简介：脚本引擎在 Microsoft Edge 中处理内存中的对象时可能触发该漏洞。成功利用该漏洞的攻击者可以获得与当前用户相同的用户权限。如果当前用户使用管理权限登录，攻击者便可以任意安装程序、查看、更改或删除数据。

3、Microsoft SharePoint 远程代码执行漏洞（CNNVD-201902-349、CVE-2019-0594）、（CNNVD-201902-391、CVE-2019-0604）

漏洞简介：当 Microsoft SharePoint 软件无法检查应用程序包的源标记时可触发该漏洞。成功利用此漏洞的攻击者可以在 SharePoint 应用程序池和 SharePoint 服务器中执行任意代码。

4 、 Microsoft Edge 内存损坏漏洞 （CNNVD-201902-400 、CVE-2019-0645）、（CNNVD-201902-378 、 CVE-2019-0650）、（CNNVD-201902-389、CVE-2019-0634）

漏洞简介：当 Microsoft Edge 不正确地访问内存中的对象时会触发该漏洞。成功利用该漏洞的攻击者可以获得与当前用户相同的用户权限，如果当前用户使用管理用户权限登录，攻击者便可以控制受影响的系统。攻击者可任意安装程序、查看、更改或删除数据、或者创建新帐户。

5 、Internet Explorer 内存损坏漏洞 （CNNVD-201902-345、CVE-2019-0606）

漏洞简介：当 Internet Explorer 不正确地访问内存中的对象时会触发该漏洞。成功利用该漏洞的攻击者可以获得与当前用户相同的用户权限，从而进一步安装程序、查看、更改或删除数据、创建新帐户。

6 、 Windows GDI 远程代码执漏洞 （CNNVD-201902-373 、CVE-2019-0662）

漏洞简介：Windows 图形设备接口 (GDI) 处理内存中对象的方式中存在远程代码执行漏洞。成功利用此漏洞的攻击者可控制受漏洞影响的系统。

7 、 Windows Office 访问连接引擎远程代码执行漏洞（CNNVD-201902-399、CVE-2019-0671）、（CNNVD-201902-401、CVE-2019-0672）、（CNNVD-201902-398 、CVE-2019-0673）、（CNNVD-201902-403、CVE-2019-0674）、（CNNVD-201902-404、CVE-2019-0675）

漏洞简介：当 Windows Office 访问连接引擎处理内存中的对象时存在远程代码执行漏洞。攻击者可以通过向目标发送经特殊设计的文件诱使其打开来利用此漏洞，成功利用此漏洞的攻击者可以在受害者系统上执行任意代码。

8、Windows DHCP 服务器远程代码执行漏洞（CNNVD-201902-372、CVE-2019-0626）

漏洞简介：当攻击者向 Windows DHCP 服务器发送经特殊设计的 DHCP 数据包时，会触发该漏洞。成功利用此漏洞的攻击者可以在服务器上执行任意代码。

安全建议

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，采取修补措施。微软官方链接地址如下：

序号	漏洞名称	官方链接
1	Microsoft Office 安全功能绕过漏洞（CNNVD-201902-356、CVE-2019-0540）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0540
2	Windows 脚本引擎内存损坏漏洞（CNNVD-201902-405、CVE-2019-0590）、（CNNVD-201902-513、CVE-2019-0591）、（CNNVD-201902-406、CVE-2019-0593）、（CNNVD-201902-385、CVE-2019-0640）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0590 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0591 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0593 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0640
3	Microsoft SharePoint 远程代码执行漏洞（CNNVD-201902-349、CVE-2019-0594）、（CNNVD-201902-391、CVE-2019-0604）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE -2019-0594 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0604
4	Microsoft Edge 内存损坏漏洞（CNNVD-201902-400、CVE-2019-0645）、（CNNVD-201902-378、CVE-2019-0650）、（CNNVD-	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0645 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0650

	201902-389 、CVE-2019-0634）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0634
5	Internet Explorer 内存损坏漏洞 （ CNNVD-201902-345 、CVE-2019-0606）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0606
6	Windows GDI 远程代码执行漏洞 （ CNNVD-201902-373 、CVE-2019-0662）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0662
7	Windows Office 访问连接引擎远程代码执行漏洞（CNNVD-201902-399 、CVE-2019-0671 ）、（CNNVD-201902-401 、CVE-2019-0672 ）、（CNNVD-201902-398 、CVE-2019-0673 ）、（CNNVD-201902-403 、CVE-2019-0674 ）、（CNNVD-201902-404 、CVE-2019-0675）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0671 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0672 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0673 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0674 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0675
8	Windows DHCP 服务器远程代码执行漏洞	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0626

	（CNNVD-201902-372 、CVE-2019-0626）	