北京师范大学网络信息安全通告

2018 年 11 月报告

北京师范大学信息网络中心

2018 年 12 月

目录

漏洞态势

根据国家信息安全漏洞库（CNNVD）统计，2018 年 11 月份采集安全漏洞共 993 个。本月接报漏洞共计 2533 个，其中信息技术产品漏洞（通用型漏洞）121 个，网络信息系统漏洞（事件型漏洞）2412 个。。

重大漏洞预警

1、macOS High Sierra 和 iOS 系统存在内核漏洞（CNNVD 编号：CNNVD-201810-1510、CVE 编号：CVE-2018-4407），该漏洞是 XNU 系统内核中网络部分的堆缓冲区溢出导致，攻击者通过向目标设备发送特殊构造的数据包从而执行恶意代码或使系统崩溃重启。触发该漏洞的必要条件是攻击者与目标系统需处于同一网络（如 Wi-Fi）。

2、微软多个安全漏洞，包括 Microsoft Internet Explorer 安全漏洞（CNNVD-201811-349、CVE-2018-8570）、Microsoft Word 安全漏洞（CNNVD-201811-387、CVE-2018-8539）、（CNNVD-201811-388、CVE-2018-8573）等多个漏洞。成功利用上述安全漏洞的攻击者，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，2018 年 11 月份新增安全漏洞共 993 个，从厂商分布来看，Apple 公司产品的漏洞数量最多，共发布 79 个；从漏洞类型来看，跨站脚本类的漏洞占比最大，达到 12.39%。本月新增漏洞中，超危漏洞 20 个、高危漏洞 76 个、中危漏洞 673 个、低危漏洞 224 个，相应修复率分别为 80.00%、86.84%、63.89%以及 56.70%。合计 639 个漏洞已有修复补丁发布，本月整体修复率 64.35%。截至 2018 年 11 月 30 日，CNNVD 采集漏洞总量已达 118613 个。

1.1. 漏洞增长概况

2018 年 11 月新增安全漏洞 993 个，与上月（1495 个）相比减少了 33.58%。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 1381 个。

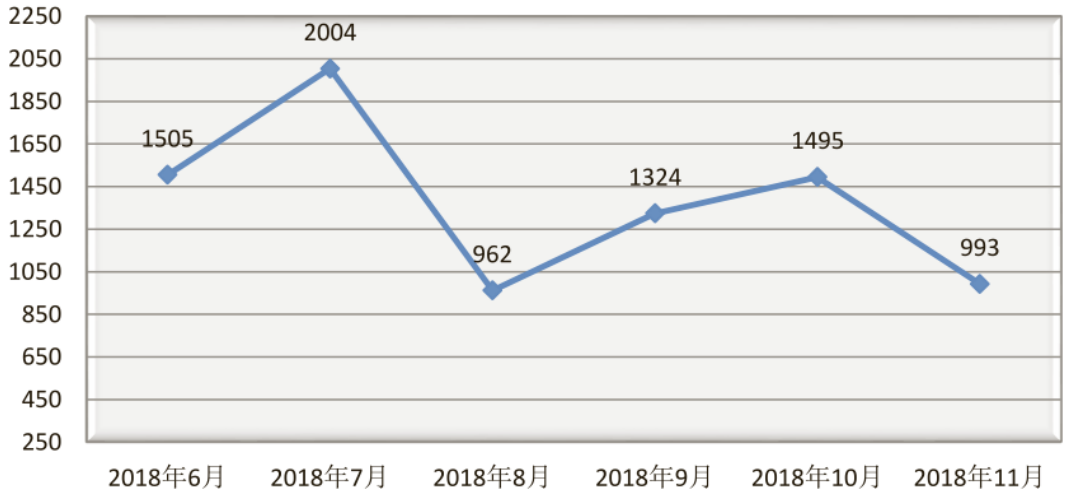

图 1 2018 年 6 月至 2018 年 11 月漏洞新增数量统计图

1.2. 漏洞分布情况

1.2.1. 漏洞厂商分布

11 月厂商漏洞数量分布情况如表 1 所示，苹果公司达到 79 个，占本月漏洞总量的 7.96%。本月苹果、谷歌、微软等公司的漏洞数量均有所上升。

表1　2018 年11 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	苹果	79	7.96%
2	谷歌	67	6.75%
3	微软	62	6.24%
4	IBM	31	3.12%
5	Terra Master	24	2.42%
6	思科	18	1.81%
7	FOSCAM	13	1.31%
8	SAP	12	1.21%
9	联想	12	1.21%
10	Apache	11	1.11%

1.2.2. 漏洞产品分布

11 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 37 条，其中桌面操作系统 36 条，服务器操作系统 32 条。本月 Android 漏洞数量最多，达到 62 个，占主流操作系统漏洞总量的 20.53%，排名第一。

表 2　2018 年 11 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	62
2	Apple High Sierra	44
3	Microsoft Windows 10	33
4	Apple iOS	32
5	Microsoft Windows Server 2016	28
6	Microsoft Windows Server 1709	17

7	Microsoft Windows Server 2012	17
8	Microsoft Windows 8.1	17
9	Microsoft Windows Rt 8.1	16
10	Microsoft Windows Server 2008	15
11	Microsoft Windows 7	15
12	Linux Kernel	6

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

11 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 12.39%。

表3　2018 年 11 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	123	12.39%
2	缓冲区错误	80	8.06%
3	SQL 注入	39	3.93%
4	权限许可和访问控制	36	3.63%
5	信息泄露	35	3.52%
6	跨站请求伪造	33	3.32%
7	命令注入	25	2.52%
8	路径遍历	21	2.11%
9	访问控制错误	9	0.91%

10	输入验证	8	0.81%
11	操作系统命令注入	6	0.60%
12	数字错误	6	0.60%
13	授权问题	5	0.50%
14	加密问题	4	0.40%
15	代码注入	3	0.30%

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。11 月漏洞危害等级分布如图 2 所示，其中超危漏洞 20 条，占本月漏洞总数的 2.01%。

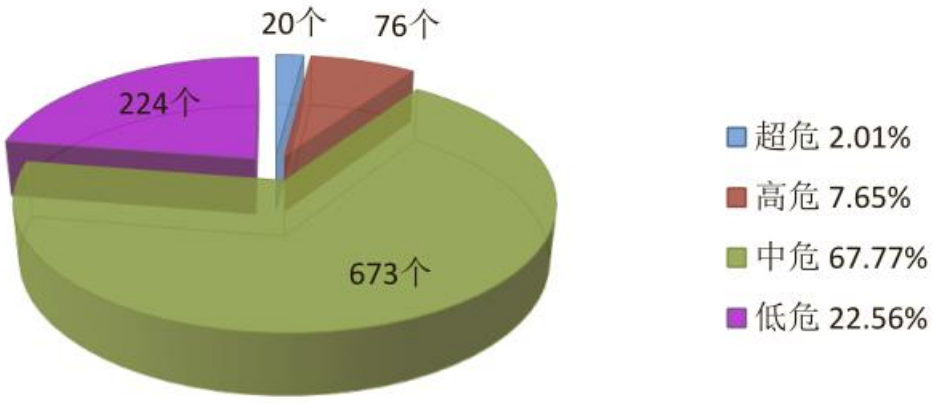

图 2　2018 年 11 月漏洞危害等级分布

1.3. 漏洞修复情况

1.3.1. 整体修复情况

11 月漏洞修复情况按危害等级进行统计见图 3。其中高危漏洞修复率最高，达到 86.84%，低危漏洞修复率最低，比例为 56.70%。与上月相比，本月中危、低危漏洞修复率有所上升，超危、高危漏洞修复率有所下降。总体来看，本月漏洞整体修复率下降，由上月的 79.53%上升至本月的 64.35%。

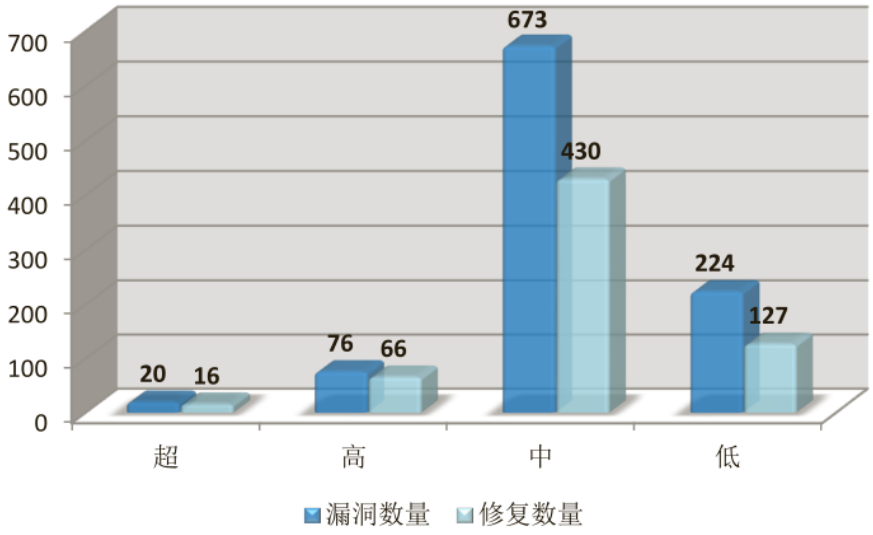

图 3　2018 年 11 月漏洞修复数量统计

1.3.2. 厂商修复情况

11 月漏洞修复情况按漏洞数量前十厂商进行统计，其中苹果、谷歌、微软等十个厂商共 329 条漏洞，占本月漏洞总数的 33.13%，漏洞修复率为 88.15%，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，其中苹果、微软、IBM、思科、SAP、联想、F5、Red Hat、戴尔、西门子等公司本月漏洞修复率均为 100%，共 417 条漏洞已全部修复。

表4　　2018 年11 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	苹果	79	79	100.00%
2	谷歌	67	66	98.51%
3	微软	62	62	100.00%
4	IBM	31	31	100.00%
5	Terra Master	24	0	0.00%
6	思科	18	18	100.00%
7	FOSCAM	13	0	0.00%
8	SAP	12	12	100.00%
9	联想	12	12	100.00%
10	Apache	11	10	90.91%

1.4. 重要漏洞实例

1.4.1. 超危漏洞实例

11 月超危漏洞共 20 个，其中重要漏洞实例如表 5 所示。

表 5 2018 年 11 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-201811-739	Ricoh	多款 RICOH Interactive Whiteboard 产品 SQL 注入漏洞（CNNVD-201811-739）
2	命令注入	CNNVD-201811-735	Ricoh	多款 RICOH Interactive Whiteboard 产品命令注入漏洞（CNNVD-201811-735）
3	缓冲区错误	CNNVD-201811-019	Schneider Electric	Schneider Electric InduSoft Web Studio 和 InTouch Edge HMI 缓冲区错误漏洞（CNNVD-201811-019）
4	访问控制错误	CNNVD-201811-179	Cisco	Cisco Stealthwatch Enterprise 访问控制错误漏洞（CNNVD-201811-179）

1. 多款 RICOH Interactive Whiteboard 产品 SQL 注入漏洞（ CNNVD-201811-739 ）

RICOH Interactive Whiteboard D2200 等都是日本理光（Ricoh）公司的多功能打印机设备。多款 RICOH Interactive Whiteboard 产品中存在 SQL 注入漏洞。远程攻击者可利用该漏洞获取或修改数据库中的信息。以下产品和版本受到影响：

- RICOH Interactive Whiteboard D2200 1.3 版本至 2.2 版本

- RICOH Interactive Whiteboard D5500 1.3 版本至 2.2 版本
- RICOH Interactive Whiteboard D5510 1.3 版本至 2.2 版本
- RICOH Interactive Whiteboard D5520（采用 RICOH InteractiveWhiteboard Controller Type1 1.3 版本至 2.2 版本或 Type2 3.0 版本至 3.1 版本）
- RICOH Interactive Whiteboard D6500（采用 RICOH InteractiveWhiteboard Controller Type1 1.3 版本至 2.2 版本）
- RICOH Interactive Whiteboard D6510（采用 RICOH InteractiveWhiteboard Controller Type1 1.3 版本至 2.2 版本或 Type2 3.0 版本至 3.1 版本）
- RICOH Interactive Whiteboard D7500（采用 RICOH InteractiveWhiteboard Controller Type1 1.3 版本至 2.2 版本或 Type2 3.0 版本至 3.1 版本）
- RICOH Interactive Whiteboard D8400（采用 RICOH InteractiveWhiteboard Controller Type1 1.3 版本至 2.2 版本或 Type2 3.0 版本至 3.1 版本）

解决措施：目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.ricoh.com/info/2018/1127_1.html

2. 多款 RICOH Interactive Whiteboard 产品命令注入漏洞（ CNNVD-201811-735 ）

RICOH Interactive Whiteboard D2200 等都是日本理光（Ricoh）公司的多功能打印机设备。多款 RICOH Interactive Whiteboard 产品中存在命令注入漏洞。远程攻击者可利用该漏洞以管理权限执行任意命令。以下产品和版本受到影响：

- RICOH Interactive Whiteboard D2200 1.6 版本至 2.2 版本
- RICOH Interactive Whiteboard D5500 1.6 版本至 2.2 版本
- RICOH Interactive Whiteboard D5510 1.6 版本至 2.2 版本

- RICOH Interactive Whiteboard D5520（采用 RICOH InteractiveWhiteboard Controller Type1 1.6 版本至 2.2 版本）

- RICOH Interactive Whiteboard D6500（采用 RICOH InteractiveWhiteboard Controller Type1 1.6 版本至 2.2 版本）

- RICOH Interactive Whiteboard D6510（采用 RICOH InteractiveWhiteboard Controller Type1 1.6 版本至 2.2 版本）

- RICOH Interactive Whiteboard D7500（采用 RICOH InteractiveWhiteboard Controller Type1 1.6 版本至 2.2 版本）

- RICOH Interactive Whiteboard D8400（采用 RICOH InteractiveWhiteboard Controller Type1 1.6 版本至 2.2 版本）

解决措施：目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.ricoh.com/info/2018/1127_1.html

3. **Schneider Electric InduSoft Web Studio Schneider Electric InduSoft Web Studio 和 InTouch Edge HMI 缓冲区错误漏洞（CNNVD-201811-019 ）**

Schneider Electric InduSoft Web Studio 和 InTouch Edge HMI（前称 InTouch Machine Edition）都是法国施耐德电气（SchneiderElectric）公司的嵌入式 HMI 软件包。该产品为 HMI 客户端提供读取、写入标签和事件监控功能。

Schneider Electric InduSoft Web Studio 8.1 SP2 之前版本和 InTouch Edge HMI 2017 SP2 之前版本中的 TCP/IP Server Task 存在基于栈的缓冲区溢出漏洞。远程攻击者可利用该漏洞执行代码。

解决措施：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.schneider-electric.com/

4. **Cisco Stealthwatch Enterprise Cisco Stealthwatch Enterprise 访问控制错误漏洞（ CNNVD-201811-179 ）**

Cisco Stealthwatch Enterprise 是美国思科（Cisco）公司的一套企业网络安全防护解决方案。该产品具有安全事件分析、网络分段管理和数据保护等功能。

Cisco Stealthwatch Enterprise 6.10.2 及之前版本中的 Stealthwatch 管理控制台（SMC）存在访问控制错误漏洞，该漏洞源于不安全的系统配置。远程攻击者可通过发送特制的 HTTP 请求利用该漏洞绕过身份验证，进而在受影响的系统上以管理权限执行任意操作。

解决措施：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-20181107-smc-auth-bypass

1.4.2. 高危漏洞实例

本月高危漏洞共 76 个，其中重点漏洞实例如表 6 所示。

表 6 2018 年 11 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-201811-275	WordPress	WordPress LearnPress SQL 注入漏洞（CNNVD-201811-275）
2	信息泄露	CNNVD-201811-603	Dell	Dell EMC Avamar Server 和EMC Integrated Data Protection Appliance 信息泄露漏洞（CNNVD-201811-603）
3	授权问题	CNNVD-201811-115 CNNVD-201811-484	Roche Siemens	Siemens SIMATIC IT LMS、SIMATIC IT Production Suite和 SIMATIC IT UA Discrete Manufacturing 授权问题

				漏洞（CNNVD-201811-484）
4	权限许可和访问控制	CNNVD-201811-117 CNNVD-201811-118	Roche	Microsoft DirectX 权限许可和访问控制漏洞（CNNVD-201811-374）
		CNNVD-201811-173	IBM	
		CNNVD-201811-182	Cisco	
		CNNVD-201811-337 CNNVD-201811-356 CNNVD-201811-369 CNNVD-201811-372 CNNVD-201811-374 CNNVD-201811-375	Microsoft	
5	缓冲区错误	CNNVD-201810-1525	Apple	TP-Link TL-R600VPN HTTPServer 缓冲区错误漏洞（CNNVD-201811-591）
		CNNVD-201811-591	普联	
		CNNVD-201811-592		
6	跨站脚本	CNNVD-201811-361	Microsoft	IBM Maximo Asset Management 跨站脚本漏洞（CNNVD-201811-740）
		CNNVD-201811-740	IBM	
7	路径遍历	CNNVD-201810-1558	Apache	Cybozu Mailwise 路径遍历漏洞（CNNVD-201811-477）
		CNNVD-201811-477 CNNVD-201811-478 CNNVD-201811-479 CNNVD-201811-480	Cybozu	
		CNNVD-201811-482	Siemens	
		CNNVD-201811-590	普联	
8	输入验证	CNNVD-201811-489 CNNVD-201811-490	Siemens	Siemens SIMATIC S7-400 输入验证漏洞（CNNVD-201811-489）

1. WordPress LearnPress SQL WordPress LearnPress SQL 注入漏洞（CNNVD-201811-275）

WordPress 是 WordPress 软件基金会的一套使用 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。LearnPress 是使用在其中的一个课程管理插件。WordPress LearnPress 3.1.0 之前版本中存在 SQL 注入漏洞。远程攻击者可利用该漏洞执行任意的 SQL 命令。

解决措施：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/learnpress/

2. Dell EMC Avamar Server Dell EMC Avamar Server 和 EMC Integrated Data Protection Appliance 信息泄露漏洞（ CNNVD- 201811-603 ）

Dell EMC Avamar Server 和 EMC Integrated Data Protection Appliance（IDPA）都是美国戴尔（Dell）公司的产品。Dell EMC Avamar Server 是一套用于服务器的完全虚拟化的备份和恢复软件。EMC Integrated Data Protection Appliance 是一套基于磁盘的备份和恢复解决方案。Dell EMC Avamar Server 和 EMC IDPA 中存在信息泄露漏洞。攻击者可利用该漏洞获取 Avamar Java 管理控制台的 SSL/TLS 私钥。以下产品和版本受到影响：

- Dell EMC Avamar Server 7.2.0 版本至 7.2.1 版本
- Dell EMC Avamar Server 7.3.0 版本至 7.3.1 版本
- Dell EMC Avamar Server 7.4.0 版本至 7.4.1 版本
- Dell EMC IDPA 2.0 版本

解决措施：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.dellemc.com/

3. Siemens SIMATIC IT LMS Siemens SIMATIC IT LMS 、e SIMATIC IT Production Suite 和 SIMATIC IT UA Discrete Manufacturing 授权问题漏洞（ CNNVD- - 201811- - 484 ）

Siemens SIMATIC IT LMS、SIMATIC IT Production Suite 和SIMATIC IT UA Discrete Manufacturing 都是德国西门子（Siemens）公司的产品。Siemens SIMATIC IT LMS 是一套总体设备效能（OEE）的线路监控系统。SIMATIC IT Production Suite 是一套工厂生产管理套件。SIMATIC IT UA Discrete Manufacturing 是一套为制造业提供结构化服务的解决方案。Siemens SIMATIC IT LMS（全部版本）、SIMATIC IT ProductionSuite 7.1 Upd3 之前的7.1版本和SIMATIC IT UA DiscreteManufacturing 2.4 之前版本中存在授权问题漏洞。攻击者可利用该漏洞绕过应用程序的身份验证检测。

解决措施：目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.plm.automation.siemens.com/global/en/support/

4. Microsoft DirectX Microsoft DirectX 权限许可和访问控制漏洞（CNNVD--201811--374）

Microsoft Windows 10 等都是美国微软（Microsoft）公司发布的一系列操作系统。DirectX 是其中的一个多媒体系统链接库。Microsoft DirectX 中存在提权漏洞，该漏洞源于程序没有正确的处理内存中的对象。本地攻击者可通过登录系统并运行特制的应用程序利用该漏洞在内核模式中执行任意代码。以下系统版本受到影响：

- Microsoft Windows 10 版本 1803
- Microsoft Windows 10 版本 1809
- Microsoft Windows Server 2019
- Microsoft Windows Server 版本 1803

解决措施：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-2018-8554

5. TP TP--Link TL--R600VPN HTTP Server 缓冲区错误漏洞（CNNVD--201811--591）

TP-Link TL-R600VPN 是中国普联（TP-LINK）公司的一款企业级路由器。HTTP Server 是其中的一个 HTTP 服务器。TP-Link TL-R600VPN FRNv1.3.0 版本（HWv3 版本）和 FRNv1.2.3 版本（HWv2 版本）中的 HTTP Server 存在缓冲区溢出漏洞。攻击者可借助特制的 IP 地址利用该漏洞执行代码或造成 HTTP server 崩溃。

解决措施：目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.tp-link.com/us/products/details/cat-4909_TL-R600VPN.html

6. IBM IBM Maximo Asset Management 跨站脚本漏洞（ CNNVD-201811-740）

IBM Maximo Asset Management 是美国 IBM 公司的一套综合性资产生命周期和维护管理解决方案。该方案能够在一个平台上管理所有类型的资产，如设施、交通运输等，并对这些资产实现单点控制。IBM Maximo Asset Management 7.6 版本中存在跨站脚本漏洞。远程攻击者可利用该漏洞在 Web UI 中注入任意 JavaScript 代码。

解决措施：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/blogs/psirt/ibm-security-bulletin-ibm-maximo-asset-management-is-vulnerable-to-cross-site-scripting-cve-2018-1584/

7. Cybozu Mailwise Cybozu Mailwise 路径遍历漏洞（ CNNVD-201811-477）

Cybozu Mailwise 是日本才望子（Cybozu）公司的一套基于 Web 的电子邮件系统。Cybozu Mailwise 5.0.0 版本至 5.4.5 版本中存在目录遍历漏洞。攻击者可利用该漏洞删除服务器上的任意文件。

解决措施：目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://kb.cybozu.support/article/34135/

8. Siemens SIMATIC S7 Siemens SIMATIC S7- - 400 输入验证漏洞（ CNNVD-201811-489 ）

Siemens SIMATIC S7-400 是德国西门子（Siemens）公司的一款用于制造和过程自动化领域的可编程逻辑控制器产品。Siemens SIMATIC S7-400 产品中存在输入验证漏洞。攻击者可借助 Ethernet 界面、PROFIBUS 或多点接口（MPI）向 TCP 102 端口发送特制的数据包利用该漏洞造成服务崩溃。以下产品和版本受到影响：

- Siemens S7-400 6 及之前版本(包括 F)
- Siemens S7-400 PN/DP 7 版本(包括 F)
- Siemens S7-400H 4.5 及之前版本
- Siemens S7-400H 6 版本
- Siemens S7-410 8.2.1 之前版本

解决措施：目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://support.industry.siemens.com/cs/ww/en/view/109476571

2. 接报漏洞情况

本月接报漏洞共计 2533 个，其中信息技术产品漏洞（通用型漏洞）121 个，网络信息系统漏洞（事件型漏洞）2412 个。

表 7 2018 年 11 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	网神信息技术（北京）股份有限公司	1065	0	1065
2	上海斗象信息科技有限公司	576	0	576
3	内蒙古奥创科技有限公司	384	31	353
4	北京数字观星科技有限公司	220	0	220
5	中新网络信息安全股份有限公司	107	3	104
6	四川虹微技术有限公司	44	0	44
7	国发中新（北京）科技发展有限公司	30	0	30
8	广州锦行网络科技有限公司	22	4	18
9	杭州迪普科技股份有限公司	22	22	0
10	浙江大华技术股份有限公司	13	12	1
11	北京西普阳光教育科技股份有限公司	11	11	0
12	北京威努特技术有限公司	7	7	0
13	北京天融信网络安全技术有限公司	6	6	0
14	中国科学院软件研究所	5	5	0

15	北京江南天安科技有限公司	5	5	0
16	亚信科技（成都）有限公司	2	2	0
17	杭州海康威视数字技术股份有限公司	2	2	0
18	沈阳汉林科技有限公司安全服务部	2	2	0
19	哈尔滨安天科技集团股份有限公司	1	1	0
20	阿里云安全	1	1	0
21	中国科学院信息工程研究所	1	1	0
22	北京安信天行科技有限公司	1	1	0
23	安徽锋刃信息科技有限公司	1	1	0
24	江苏通付盾科技有限公司	1	1	0
25	北京兰云科技有限公司	1	1	0
26	西安交大捷普网络科技有限公司	1	1	0
27	MANIS 团队	1	1	0
28	北京中科物安科技有限公司	1	1	0
报送总计		2533	121	2412

3. 重大漏洞预警

3.1. 关于 macOS 和 和 iOS 内核漏洞的通报

本月 CNNVD 收到关于 macOS 和 iOS 内核漏洞（CNNVD 编号：CNNVD-201810-1510、CVE 编号：CVE-2018-4407）情况的报送。成功利用漏洞的攻击者可能对目标系统执行恶意代码或使系统崩溃重启。iOS11 及其以下版本、MacOS High Sierra 10.13.6 及其以下版本的设备均受此漏洞影响。目前，苹果官方已经发布了版本更新修复了该漏洞。建议用户及时确认系统版本，如受影响，请及时采取修补措施。

漏洞简介

macOS High Sierra 是 2017 年 6 月苹果公司在 WWDC 开发者大会上发布的苹果桌面操作系统，iOS 是由美国苹果公司开发的应用于苹果手机、平板等设备的操作系统。

macOS High Sierra 和 iOS 系统存在内核漏洞（CNNVD 编号：CNNVD-201810-1510、CVE 编号：CVE-2018-4407），该漏洞是 XNU 系统内核中网络部分的堆缓冲区溢出导致，攻击者通过向目标设备发送特殊构造的数据包从而执行恶意代码或使系统崩溃重启。触发该漏洞的必要条件是攻击者与目标系统需处于同一网络（如 Wi-Fi）。

漏洞危害

成功利用该漏洞的攻击者，可以在目标系统中执行恶意代码。iOS11 及其以下版本、MacOS High Sierra 10.13.6 及其以下版本的设备均受此漏洞影响。

修复措施

目前，苹果官方已经发布了版本更新修复了该漏洞。建议用户及时确认系统版本，如受影响，请及时采取修补措施。漏洞修补措施如下：

1、进行系统更新，更新到最新版本

2、如果没有更新到最新版本，可在 macOS 防火墙中启用隐藏模式可防止攻击。这个系统设置默认情况下不启用，需要用户手动开启。

3.2. 关于微软多个安全漏洞情况的通报

本月微软官方发布了多个安全漏洞的公告，包括 Microsoft Internet Explorer 安全漏洞（CNNVD-201811-349、CVE-2018-8570）、Microsoft Word 安全漏洞（CNNVD-201811-387、CVE-2018-8539）、（CNNVD-201811-388、CVE-2018-8573）等多个漏洞。成功利用上述安全漏洞的攻击者，可以在目标系统上执行任意代码。微软多个产品和系统受漏洞影响。目前，微软官方已经发布补丁修复了上述漏洞，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

漏洞介绍

本次漏洞公告涉及 Microsoft Internet Explorer 、MicrosoftOutlook 、Microsoft Word 、Microsoft Excel 、Microsoft Project 、Microsoft JScriptMicrosoft SharePoint 、Microsoft PowerShell、Windows TFTP 服务器、Chakra 脚本引擎、Windows 内核、MicrosoftDynamics 365 等 Windows 平台下应用软件和组件。漏洞详情如下：

1、Internet Explorer 安全漏洞（CNNVD-201811-349、CVE-2018-8570）

漏洞简介：Internet Explorer 部分版本存在远程代码执行漏洞，当 Internet Explorer 不正确地访问内存中的对象时，可触发该漏洞。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。

2、Microsoft Outlook 安全漏洞（CNNVD-201811-376、CVE-2018-8522）、（CNNVD-201811-378、CVE-2018-8524）、（CNNVD-201811-377、CVE-2018-8576）、（CNNVD-201811-379、CVE-2018-8582）

漏洞简介：当 Microsoft Outlook 软件无法正确处理内存中的对象时，就会触发该漏洞。攻击者可以向目标系统发送经过特殊设计的文件，从而在当前用户权限下执行恶意代码。

3、Microsoft Word 安全漏洞（CNNVD-201811-387、CVE-2018-8539）、（CNNVD-201811-388、CVE-2018-8573）

漏洞简介：当 Microsoft Word 软件无法正确处理内存中的对象时，就会触发该漏洞。攻击者必须诱使用户使用 Microsoft Word 打开经特殊设计的文件，才能利用此漏洞。成功利用此漏洞的攻击者可以在当前用户权限下执行恶意代码。

4、Microsoft Excel 安全漏洞（CNNVD-201811-385、CVE-2018-8574）、（CNNVD-201811-386、CVE-2018-8577）

漏洞简介：当 Microsoft Excel 软件无法正确处理内存中的对象时，就会触发该漏洞。攻击者必须诱使用户使用 Microsoft Excel 打开经特殊设计的文件，才能利用此漏洞。成功利用此漏洞的攻击者可以在当前用户权限下执行恶意代码。

5、Microsoft JScript 安全漏洞（CNNVD-201811-360、CVE-2018-8417）

漏洞简介：Microsoft JScript 中存在可能允许攻击者绕过 DeviceGuard 的安全功能的漏洞，攻击者通过访问本地计算机，然后运行经特殊设计的应用程序从而创建任意 COM 对象。

6、Windows Search 安全漏洞（CNNVD-201811-362、CVE-2018-8450）

漏洞简介：如果 Windows Search 无法正确处理内存中的对象，就会触发该漏洞。攻击者需要向 Windows Search 服务发送经特殊设计的消息，从而执行恶意文件。

7、Microsoft PowerShell 安全漏洞（CNNVD-201811-347、CVE-2018-8256）、（CNNVD-201811-358、CVE-2018-8415）

漏洞简介：如果 Microsoft PowerShell 无法正确处理内存中的对象，可能就会触发该漏洞。攻击者可以向目标系统发送经过特殊设计的文件，从而执行恶意文件。

8、Microsoft SharePoint 权限提升漏洞（CNNVD-201811-382、CVE-2018-8568）、（CNNVD-201811-383、CVE-2018-8572）

漏洞简介：当 Microsoft SharePoint Server 没有正确地处理发往 SharePoint 服务器的 Web 请求时，就会触发该漏洞。经过身份验证的攻击者

可能通过向受影响的 SharePoint 服务器发送经特殊设计的请求来利用此漏洞，从而执行恶意文件。

9、Microsoft Project 安全漏洞（CNNVD-201811-371、CVE-2018-8575）

漏洞简介：当 Microsoft Project 软件无法正确处理内存中的对象时，就会触发该漏洞。攻击者可能通过向用户发送经特殊设计的文件并诱使用户打开，从而执行恶意代码。

10、Windows 内核信息泄漏漏洞（CNNVD-201811-355、CVE-2018-8408））

漏洞简介：当 Windows 内核不正确地处理内存中的对象时会触发该漏洞。成功利用此漏洞的攻击者可以获取信息，从而进一步入侵用户系统。已经过身份验证的攻击者可以通过运行经特殊设计的应用程序来利用此漏洞。

11、Windows TFTP 服务器安全漏洞（CNNVD-201811-341、CVE-2018-8476）

漏洞简介：Windows 部署服务 TFTP 服务器在处理内存中的对象时存在远程代码执行漏洞。攻击者可以创建经特殊设计的请求，提升 Windows 权限，从而执行恶意代码。

12、Chakra 脚本引擎安全漏洞（CNNVD-201811-338、CVE-2018-8541）、（CNNVD-201811-339、CVE-2018-8542）、（CNNVD-201811-390、CVE-2018-8543）（CNNVD-201811-340、CVE-2018-8551）、（CNNVD-201811-342、CVE-2018-8555）、（CNNVD-201811-345、CVE-2018-8556）、（CNNVD-201811-346、CVE-2018-8557）、（CNNVD-201811-348、CVE-2018-8588）

漏洞简介：Chakra 脚本引擎在 Microsoft Edge 中处理内存中的对象的时可能触发该漏洞。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。

13、Windows 权限提升漏洞（CNNVD-201811-373、CVE-2018-8592）

漏洞简介：如果在系统上使用物理介质（USB、DVD 等）安装程序，并在安装过程中选择了“不保留任何内容”选项，就会触发 Windows 10 版本 1809

中的权限提升漏洞。成功利用此漏洞的攻击者可以在受影响系统上获得本地访问权限。

14、Microsoft Dynamics 365 版本 8 安全漏洞（CNNVD-201811-396、CVE-2018-8609）

漏洞简介：当 Dynamics 服务器无法正确清理 Web 请求时，就会触发该漏洞。经过身份验证的攻击者可以通过向目标 Dynamics 服务器发送特殊构造的请求来利用此漏洞，从而在目标服务器上执行恶意代码。

漏洞危害

成功利用上述安全漏洞的攻击者，可以在目标系统上执行任意代码。微软多个产品和系统受漏洞影响。

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，尽快采取修补措施。微软官方链接地址如下：

1. Microsoft Internet Explorer 安全漏洞（CNNVD-201811-349、CVE-2018-8570）

官方链接地址：https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8570

2. Microsoft Outlook 安全漏洞（CNNVD-201811-376、CVE-2018-8522）、（CNNVD-201811-378、CVE-2018-8524）、（CNNVD-201811-377、CVE-2018-8576）、（CNNVD-201811-379、CVE-2018-8582）

官方链接地址：https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8522

https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8524

https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8576

https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8582

3. Microsoft Word 安全漏洞（CNNVD-201811-387 、CVE-2018-8539） 、（CNNVD-201811-388 、CVE-2018-8573）

官方链接地址：https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8539

https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8573

4. Microsoft Excel 安全漏洞（CNNVD-201811-385 、CVE-2018-8574） 、（CNNVD-201811-386 、CVE-2018-8577）

官方链接地址：https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8574

https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8577

5. Microsoft JScript 安全漏洞（ CNNVD-201811-360 、CVE-2018-8417）

官方链接地址：https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8417

6. Windows Search 安全漏洞（CNNVD-201811-362 、CVE-2018-8450）

官方链接地址：https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8450

7. Microsoft PowerShell 安全漏洞（CNNVD-201811-347 、CVE-2018-8256）、（CNNVD-201811-358 、CVE-2018-8415）

官方链接地址：https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8256

https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8415

8. Microsoft SharePoint 权限提升漏洞（CNNVD-201811-382 、CVE-2018-8568） 、（CNNVD-201811-383 、CVE-2018-8572）

官方链接地址：https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8568

https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8576

9. Microsoft Project 安全漏洞（ CNNVD-201811-371 、CVE-2018-8575）

官方链接地址：https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8576

10. Windows 内核信息泄漏漏洞（ CNNVD-201811-355 、CVE-2018-8408）

官方链接地址：https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8408

11. Windows TFTP 服务器安全漏洞 （ CNNVD-201811-341 、CVE-2018-8476）

官方链接地址：https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8476

12. Chakra 脚本引擎安全漏洞（ CNNVD-201811-338 、CVE-2018-8541 ） 、（ CNNVD-201811-339 、CVE-2018-8542 ） 、（ CNNVD-201811-390 、CVE-2018-8543 ）（ CNNVD-201811-340 、CVE-2018-8551 ） 、（ CNNVD-201811-342 、CVE-2018-8555 ） 、（ CNNVD-201811-345 、CVE-2018-8556 ） 、（ CNNVD-201811-346 、CVE-2018-8557 ） 、（ CNNVD-201811-348 、CVE-2018-8588）

官方链接地址：https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8541

https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8542

https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8543

https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8551

https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8555

https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8556

https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8557

https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8588

13. Windows 权限提升漏洞（ CNNVD-201811-373 、CVE-2018-8592）

官方链接地址：https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8592

14. Microsoft Dynamics 365 版本 8 安全漏洞（CNNVD-201811-396、CVE-2018-8609）

官方链接地址：https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8609