北京师范大学网络信息安全通告

2018 年 12 月报告

北京师范大学信息网络中心

2019 年 1 月

目录

漏洞态势

根据国家信息安全漏洞库（CNNVD）统计，2018 年 12 月份采集安全漏洞共 1275 个。本月接报漏洞共计 3629 个，其中信息技术产品漏洞（通用型漏洞）76 个，网络信息系统漏洞（事件型漏洞）3553 个。

重大漏洞预警

微软多个安全漏洞，包括 Microsoft Internet Explorer 安全漏洞（CNNVD-201812-458、CVE-2018-8619）、Microsoft Excel 安全漏洞（CNNVD-201812-466、CVE-2018-8597）等多个漏洞。成功利用上述漏洞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。

1. 公开漏洞情况

根据国家信息安全漏洞库（CNNVD）统计，2018 年 12 月份新增安全漏洞共 1275 个，从厂商分布来看，谷歌公司产品的漏洞数量最多，共发布 97 个；从漏洞类型来看，缓冲区错误类的漏洞占比最大，达到 15.37%。本月新增漏洞中，超危漏洞 24 个、高危漏洞 97 个、中危漏洞 855 个、低危漏洞 299 个，相应修复率分别为 87.50%、84.54%、75.32%以及 69.57%。合计 955 个漏洞已有修复补丁发布，本月整体修复率 74.90%。截至 2018 年 12 月 31 日，CNNVD 采集漏洞总量已达 119892 个。

1.1. 漏洞增长概况

2018 年 12 月新增安全漏洞 1275 个，与上月（993 个）相比增加了 28.40%。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 1342 个。

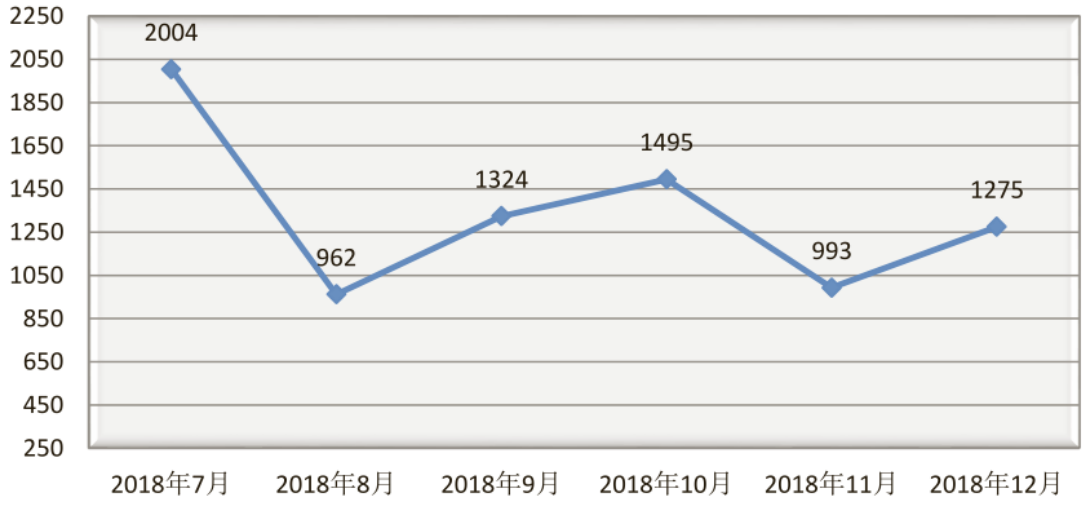

图 1 2018 年 7 月至 2018 年 12 月漏洞新增数量统计图

1.2. 漏洞分布情况

1.2.1. 漏洞厂商分布

12 月厂商漏洞数量分布情况如表 1 所示，谷歌公司达到 97 个，占本月漏洞总量的 7.61%。本月 Adobe、谷歌、IBM 等公司的漏洞数量均有所上升，微软的漏洞数量出现下降。

表1 2018 年12 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	谷歌	97	7.61%
2	Adobe	91	7.14%
3	IBM	72	5.65%
4	微软	40	3.14%
5	Qualcomm	39	3.06%
6	Infovista	26	2.04%
7	Apple	25	1.96%
8	Schneider Electric	22	1.73%
9	WordPress	16	1.25%
10	华芸科技	15	1.18%

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 Windows 系列操作系统漏洞数量共 26 条，其中桌面操作系统 26 条，服务器操作系统 22 条。本月 Android 漏洞数量最多，达到 47 个，占主流操作系统漏洞总量的 23.15%，排名第一。

表 2 2018 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	47
2	Microsoft Windows 10	24
3	Apple iOS	20
4	Microsoft Windows Server 2016	20
5	Microsoft Windows Server 2012	15
6	Microsoft Windows Server 2008	14
7	Microsoft Windows 7	14
8	Microsoft Windows 8.1	13
9	Microsoft Windows Rt 8.1	13
10	Microsoft Windows Server 1709	11
11	Linux Kernel	7
12	Apple macOS High Sierra	5

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

12 月份发布的漏洞类型分布如表 3 所示，其中缓冲区错误类漏洞所占比例最大，约为 15.37%。

表3　2018 年 12 月漏洞类型统计表

序号	漏洞类型	漏洞数量	所占比例
1	缓冲区错误	196	15.37%

2	跨站脚本	173	13.57%
3	信息泄露	59	4.63%
4	权限许可和访问控制	35	2.75%
5	输入验证	29	2.27%
6	SQL 注入	25	1.96%
7	路径遍历	22	1.73%
8	跨站请求伪造	20	1.57%
9	访问控制错误	15	1.18%
10	操作系统命令注入	14	1.10%
11	数字错误	13	1.02%
12	命令注入	9	0.71%
13	授权问题	3	0.24%
14	代码注入	3	0.24%
15	加密问题	2	0.16%
16	竞争条件	2	0.16%
17	资源管理错误	2	0.16%
18	注入	1	0.08%
19	配置错误	1	0.08%

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 3 所示，其中超危漏洞 24 条，占本月漏洞总数的 1.88%。

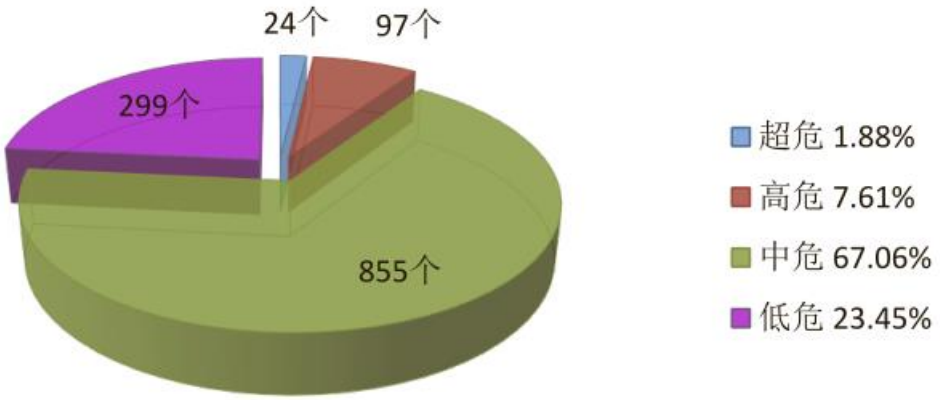

图 2　2018 年 12 月漏洞危害等级分布

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。其中超危漏洞修复率最高，达到 87.50%，低危漏洞修复率最低，比例为 69.57%。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，本月整体修复率上升，由上月的 64.35%上升至本月的 74.90%。

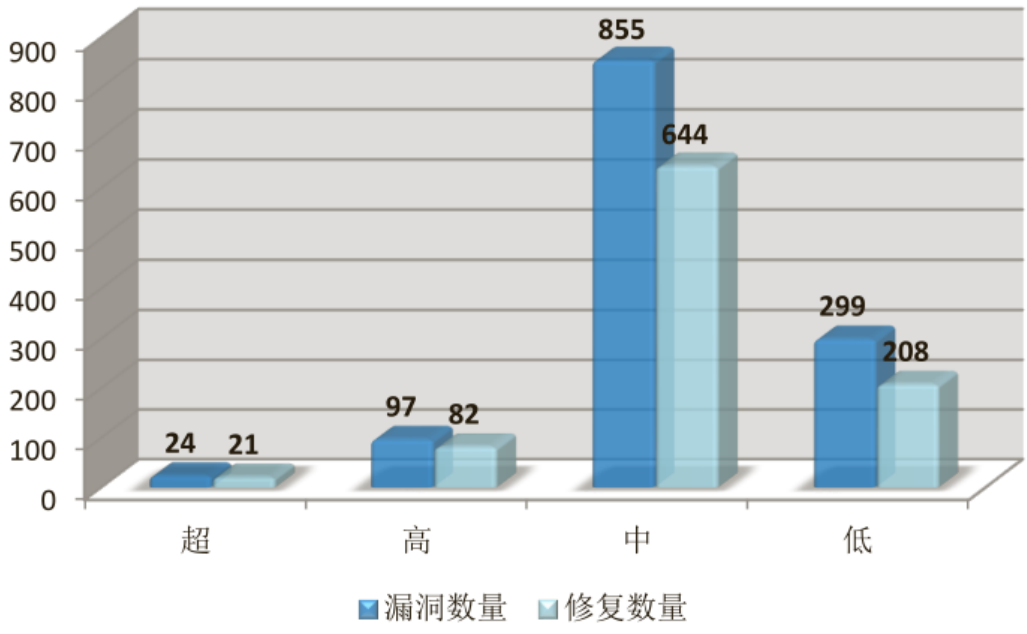

图 3　2018 年 12 月漏洞修复数量统计

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 Apple、Google、Microsoft 等十个厂商共 443 条漏洞，占本月漏洞总数的 34.75%，漏洞修复率为 98.65%，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 Google、Adobe、IBM、Microsoft、Qualcomm、Infovista、Apple、华芸科技、Siemens、Mozilla 等公司本月漏洞修复率均为 100%，共 636 条漏洞已全部修复。

表 4 2018 年 12 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	Google	97	97	100.00%
2	Adobe	91	91	100.00%
3	IBM	72	72	100.00%
4	Microsoft	40	40	100.00%
5	Qualcomm	39	39	100.00%
6	Infovista	26	26	100.00%
7	Apple	25	25	100.00%
8	SchneiderElectric	22	19	86.36%
9	WordPress	16	13	81.25%
10	华芸科技	15	15	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 24 个，其中重要漏洞实例如表 5 所示。

表 5 2018 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	操作系统命令	CNNVD-201812-004 CNNVD-201812-090 CNNVD-201812-095 CNNVD-201812-099 CNNVD-201812-100	NUUO、华芸科技	NUUO NVRMini2 操作系统命令漏洞（CNNVD-201812-004）
2	缓冲区错误	CNNVD-201812-598 CNNVD-201812-724 CNNVD-201812-866	Siemens、Webroot、Wibu-Systems	Wibu-Systems WibuKey server management 缓冲区错误漏洞（CNNVD-201812-866）
3	访问控制错误	CNNVD-201812-788	3S-Smart Software Solutions	多款 3S-Smart Software Solutions 产品访问控制错误漏洞（CNNVD-201812-788）
4	路径遍历	CNNVD-201812-402	Cybozu	Cybozu Remote Service 路径遍历漏洞（CNNVD-201812-402）
5	输入验证	CNNVD-201811-832 CNNVD-201812-096 CNNVD-201812-1094	Qualcomm、华芸科技、Schneider Electric	Schneider Electric Pro-Face GP-Pro EX 输入验证漏洞（CNNVD-201812-1094）

1. NUUO NVRMini2 是 NUUO 公司的一款小型网络硬盘录像机设备

NUUO NVRMini2 3.10.0 及之前版本中存在命令注入漏洞。远程攻击者可通过向 upgrade_handle.php 文件发送特制的请求利用该漏洞以 root 身份执行操作系统命令。

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.nuuo.com/

2. Wibu Wibu-Systems WibuKey server management 缓冲区错误漏洞（CNNVD-201812-866）

Wibu-Systems WibuKey 是德国威步（Wibu-Systems）公司的一套数字版权管理（DRM）解决方案。Network server management 是其中的一个网络服务器管理器。

Wibu-Systems WibuKey 6.40.2402.500 版本中的 servermanagement 的‘WkbProgramLow’函数存在堆溢出漏洞。攻击者可通过发送畸形的 TCP 数据包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.wibu.com/

3. 多款 3S-Smart Software Solutions 产品访问控制错误漏洞（CNNVD-201812-788）

3S-Smart CODESYS Control for BeagleBone 等都是德国 3S-Smart Software Solutions 公司的用于工业控制系统开发的编程软件。多款 3S-Smart Software Solutions 产品中存在访问控制错误漏洞，该漏洞源于默认情况下程序没有启用用户访问管理和通信加密。攻击者可利用该漏洞访问设备和敏感信息，包括用户凭证。以下产品受到影响：

-3S-Smart CODESYS Control for BeagleBone

-3S-Smart CODESYS Control for emPC-A/iMX6

-3S-Smart CODESYS Control for IOT2000

-3S-Smart CODESYS Control for Linux

-3S-Smart CODESYS Control for PFC100

-3S-Smart CODESYS Control for PFC200

-3S-Smart CODESYS Control for Raspberry Pi

-3S-Smart CODESYS Control RTE V3

-3S-Smart CODESYS Control RTE V3（用于 Beckhoff CX）

-3S-Smart CODESYS Control Win V3（CODESYS setup 的组成部分）

-3S-Smart CODESYS V3 Simulation Runtime（CODESYS Development System 的组成部分）

-3S-Smart CODESYS Control V3 Runtime System Toolkit

-3S-Smart CODESYS HMI V3

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.codesys.com/fileadmin/data/customers/security/2018/Advisory2018-10_CDS-61037.pdf

4. Cybozu Remote Service 路径遍历漏洞（CNNVD-201812-402）

Cybozu Remote Service 是日本才望子（Cybozu）公司的一套用于访问才望子（Cybozu）内部系统的远程服务管理软件。Cybozu Remote Service 3.0.0 版本至 3.1.8 版本中的 used devicemanagement 页面存在目录遍历漏洞。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/34301/

5. Schneider Electric Pro-Face GP-Pro EX 输入验证漏洞（CNNVD-201812-1094）

Schneider Electric Pro-Face GP-Pro EX 是法国施耐德电气（Schneider Electric）公司的一套 HMI 界面编辑和逻辑编程软件。Schneider Electric Pro-Face GP-Pro EX 4.08 及之前版本中存在输入验证漏洞。攻击者可利用该漏洞在 GP-Pro EX 启动时执行任意可执行文件。

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://www.schneider-electric.com/en/download/document/SEVD-2018-354-02/

1.4.2. 高危漏洞实例

本月高危漏洞共 97 个，其中重点漏洞实例如表 6 所示。

表 6 2018 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-201811-853	Cisco	Cisco Prime License Manager SQL 注入漏洞（CNNVD-201811-853）
2	信息泄露	CNNVD-201812-707	NEC	NEC Aterm WF1200CR 和 Aterm WG1200CR 信息泄露漏洞（CNNVD-201812-707）
3	授权问题	CNNVD-201812-785	ABB	ABB CMS-770 授权问题漏洞（CNNVD-201812-785）
4	操作系统命令注入	CNNVD-201812-267 CNNVD-201812-268	摩莎	Moxa NPort W2x50A 操作系统命令注入漏洞（CNNVD-201812-267）
		CNNVD-201812-657	Geutebrück	Geutebrück E2 Camera Series 操作系统命令注入漏洞（CNNVD-201812-657）
		CNNVD-201812-810	TOSHIBA	TOSHIBA Home Gateway HEM-GW26A 和 TOSHIBA Home Gateway HEM-GW16A 操作系统命令注入漏洞（CNNVD-201812-810）
5	权限许可和访问控制	CNNVD-201812-039	Brocade	Microsoft Windows 权限许可和访问控制漏洞（CNNVD-201812-442）
		CNNVD-201812-064	Red Hat	
		CNNVD-201812-247	Google	
		CNNVD-201812-442	Microsoft	
		CNNVD-201812-443		
		CNNVD-201812-462		
		CNNVD-201812-817	IBM	

		CNNVD-201812-818	Cisco	
6	跨站脚本	CNNVD-201811-833 CNNVD-201811-837 CNNVD-201811-838 CNNVD-201811-839 CNNVD-201811-841 CNNVD-201811-829	Qualcomm	Apple macOS Mojave Intel Graphics Driver 缓冲区错误漏洞（CNNVD-201812-208）
		CNNVD-201811-863	IBM	
		CNNVD-201811-921	HPE	
		CNNVD-201812-208	Apple	
		CNNVD-201812-317	Google	
		CNNVD-201812-659	Schneider Electric	
		CNNVD-201812-604	Siemens	
		CNNVD-201812-748	Swisscom	
		CNNVD-201812-789	研华	
		CNNVD-201812-924	Google	
7	访问控制错误	CNNVD-201811-830	Qualcomm	多款 Qualcomm Snapdragon产品访问控制错误漏洞（CNNVD-201811-835）
		CNNVD-201811-835		
8	路径遍历	CNNVD-201812-052	Drobo	ASUSTOR ADM 路径遍历漏洞（CNNVD-201812-097）
		CNNVD-201812-097	华芸科技	
		CNNVD-201812-403	Cybozu	
		CNNVD-201812-656	GE	
		CNNVD-201812-1095	Schneider Electric	
9	输入验证	CNNVD-201811-831	Qualcomm	多款 Qualcomm Snapdragon 产品输入验证漏洞（CNNVD-201811-831）
10	配置错误	CNNVD-201812-923	Google	Android Boot 配置错误漏洞（CNNVD-201812-

				923）

1. Cisco Prime License Manager SQL 注入漏洞（CNNVD-201811-853）

Cisco Prime License Manager（PLM）是美国思科（Cisco）公司的一款许可证管理器。Cisco PLM 11.0.1 及之后版本中的 web 框架代码存在 SQL 注入漏洞，该漏洞源于程序对 SQL 查询语句中用户提交的输入缺少适当的验证。远程攻击者可通过发送特制的 HTTP POST 请求利用该漏洞修改和删除 PLM 数据库中的任意数据，或获取 shell 访问权限。

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-20181128-plm-sql-inject

2. NEC Aterm WF1200CR 和 Aterm WG1200CR 信息泄露漏洞（CNNVD-201812- 707）

NEC Aterm WF1200CR 和 Aterm WG1200CR 都是日本电气（NEC）公司的路由器产品。使用 1.1.1 及之前版本固件的 NEC Aterm WF1200CR 和使用 1.0.1 及之前版本固件的 Aterm WG1200CR 中存在信息泄露漏洞。攻击者可利用该漏洞获取设备上的注册信息。

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://jpn.nec.com/security-info/secinfo/nv18-021.html

3.ABB CMS-770 授权问题漏洞（CNNVD-201812-785）

ABB CMS-770 是瑞士 ABB 公司的一套电路监控系统。ABB CMS-770 1.7.1 及之前版本中存在授权问题漏洞。攻击者可利用该漏洞读取敏感的配置文件。

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：http://search-ext.abb.com/library/Download.aspx?DocumentID=ABBVU-

EPBP-R-5673&LanguageCode=en&DocumentPartId=2CKA008100A0351%3B%202CCA688307R0001&Action=Launch

4. Moxa NPort W2x50A 操作系统命令注入漏洞（CNNVD-201812-267）

Moxa NPort W2x50A 是摩莎（Moxa）公司的一款用于将工业串口设备连上网络的串口通讯服务器。使用 2.2 Build_18082311 之前版本固件的 Moxa NPort W2x50A 产品中的 web server ping 功能存在操作系统命令注入漏洞。攻击者可通过向/goform/net_WebPingGetValue 发送特制的 HTTP POST 请求利用该漏洞以 root 用户身份运行操作系统命令。

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.moxa.com/

5. Microsoft Windows 权限许可和访问控制漏洞（CNNVD-201812-4422）

Microsoft Windows 10 等都是美国微软（Microsoft）公司发布的一系列操作系统。Microsoft Windows 10 是一套个人电脑使用的操作系统。Windows Server 2008 SP2 是一套服务器操作系统。Microsoft Windows 中存在提权漏洞，该漏洞源于 Windows 内核模式驱动程序未能正确处理内存中的对象。攻击者可利用该漏洞在内核模式中运行任意代码。以下版本受到影响：

- 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 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 1709
- 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-2018-8641

6.Apple macOS Mojave Intel Graphics Driver 缓冲区错误漏洞（CNNVD-201812-208）

Apple macOS Mojave 是美国苹果（Apple）公司的一套专为 Mac 计算机所开发的专用操作系统。Intel Graphics Driver 是其中的一个集成显卡驱动程序。Apple macOS Mojave 10.14.1 版本中的 Intel Graphics Driver 组件存在越界读取漏洞。本地攻击者可利用该漏洞造成系统意外终止或读取内存内容。

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.apple.com/zh-cn/HT209341

7. 多款 n Qualcomm Snapdragon 产品访问控制错误漏洞（CNNVD-201811-835）

Qualcomm MDM9206 等都是美国高通（Qualcomm）公司产品。Qualcomm MDM9206 是一款中央处理器（CPU）。SDX24 是一款调制解调器。多款 Qualcomm Snapdragon 产品中的内核存在访问控制错误漏洞。攻击者可利用该漏洞执行未授权的操作。以下产品（用于汽车、移动和可穿戴设备）受到影响：

- Qualcomm MDM9206
- Qualcomm MDM9607
- Qualcomm MDM9650
- Qualcomm MSM8996AU
- Qualcomm SD 210
- Qualcomm SD 212
- Qualcomm SD 205
- Qualcomm SD 425
- Qualcomm SD 430
- Qualcomm SD 450
- Qualcomm SD 625
- Qualcomm SD 820
- Qualcomm SD 820A
- Qualcomm SD 835
- Qualcomm SD 845
- Qualcomm SD 850
- Qualcomm SDA660
- Qualcomm SDA845
- Qualcomm SDX24
- Qualcomm SXR1130

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.qualcomm.com/company/product-security/bulletins

8. ASUSTOR ADM 路径遍历漏洞（ CNNVD-201812-097 ）

ASUSTOR ADM 是华芸科技（ASUSTOR）公司的一套专用于 ASUSTOR NAS 存储设备的操作系统。ASUSTOR ADM 3.1.1 版本中的 downloadwallpaper.cgi 文件存在目录遍历漏洞。攻击者可通过操纵‘file’和‘folder’URL 参数利用该漏洞下载任意文件。

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.asustor.com/

9. 多款 Qualcomm Snapdragon 产品输入验证漏洞（CNNVD-201811-831）

Qualcomm MSM8996AU 等都是美国高通（Qualcomm）公司的用于不同平台的中央处理器（CPU）产品。多款 Qualcomm Snapdragon 产品中的 SafeSwitch 存在输入验证漏洞。攻击者可利用该漏洞绕过与调制解调器相关的限制。以下产品（用于汽车和移动设备）受到影响：

- Qualcomm MSM8996AU
- Qualcomm SD 410/12
- Qualcomm SD 820
- Qualcomm SD 820A

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.qualcomm.com/company/product-security/bulletins

10. Android Boot 配置错误漏洞（CNNVD-201812-923）

Android 是美国谷歌（Google）公司和开放手持设备联盟（简称 OHA）共同开发的一套以 Linux 为基础的开源操作系统。Boot 是一款移植工具。Android 中的 Boot 存在配置错误漏洞。攻击者可利用该漏洞在系统上执行任意代码或造成应用程序崩溃。

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.codeaurora.org/security-bulletin/2018/12/03/december-2018-code-aurora-security-bulletin

2. 接报漏洞情况

本月接报漏洞共计 3629 个，其中信息技术产品漏洞（通用型漏洞）76 个，网络信息系统漏洞（事件型漏洞）3553 个。

表 7　2018 年 12 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	1477	0	1477
2	网神信息技术（北京）股份有限公司	1349	0	1349
3	中新网络信息安全股份有限公司	215	0	215
4	北京数字观星科技有限公司	157	0	157
5	新华三技术有限公司	131	0	131
6	内蒙古奥创科技有限公司	102	4	98
7	四川虹微技术有限公司	27	0	27
8	北京圣博润高新技术股份有限公司	26	0	26
9	西安四叶草信息技术有限公司	22	22	0
10	国发中新（北京）科技发展有限公司	24	0	24
11	北京锦龙信安科技有限公司	20	0	20
12	广州锦行网络科技有限公司	18	3	15
13	浙江大华技术股份有限公司	13	12	1
14	西安交大捷普网络科技有限公司	12	1	11

15	北京天融信网络安全技术有限公司	11	11	0
16	中国科学院软件研究所	6	6	0
17	个人	4	3	1
18	杭州海康威视数字技术股份有限公司	2	2	0
19	北京江南天安科技有限公司	2	2	0
20	厦门服云信息科技有限公司	2	2	0
21	广州市昊恒科技有限公司	2	2	0
22	亚信科技（成都）有限公司	2	2	0
23	上海大学机电工程与自动化学院	1	1	0
24	北京启明星辰信息安全技术有限公司	1	1	0
25	山东华鲁科技发展股份有限公司	1	1	0
26	安徽锋刃信息科技有限公司	1	1	0
27	天懋信息	1	0	1
报送总计		3629	76	3553

3. 重大漏洞预警

3.1. CNNVD 关于微软多个安全漏洞情况的通报

近日，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-201812-458、CVE-2018-8619）、Microsoft Excel 安全漏洞（CNNVD-201812-466、CVE-2018-8597）等多个漏洞。成功利用上述漏洞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 Internet Explorer 、MicrosoftOutlook 、Microsoft Excel 、Microsoft PowerPoint 、Microsoft VBScript、Chakra 脚本引擎、.NET Framework、Microsoft 文本到语音转换等 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-201812-458 、CVE-2018-8619）

漏洞简介：Internet Explorer 部分版本存在远程代码执行漏洞，当 Internet Explorer VBScript 执行策略未正确限制 VBScript 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-201812-469 、CVE-2018-8587）

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 Excel 安全漏洞（CNNVD-201812-466、 CVE-2018-8597）、（CNNVD-201812-446、 CVE-2018-8636）

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。

4 、 Microsoft PowerPoint 安全漏洞（CNNVD-201812-451、CVE-2018-8628）

漏洞简介：当 Microsoft PowerPoint 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 PowerPoint 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 VBScript 安全漏洞（CNNVD-201812-454、CVE-2018-8625）

漏洞简介：当 Microsoft VBScript 引擎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 Internet Explorer 打开经特殊设计的网页或诱使用户使用 Microsoft Office 打开嵌入经特殊设计的 ActiveX 控件的文档等，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。

6、Microsoft .NET Framework 安全漏洞（CNNVD-201812-472 、CVE-2018-8540）

漏洞简介：当 Microsoft .NET Framework 处理不受信任的输入时可能会触发该漏洞。成功利用漏洞的攻击者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、或者创建新帐户等。

7、Microsoft 文本到语音转换程序安全漏洞（CNNVD-201812-448、CVE-2018-8634）

漏洞简介：当 Microsoft 文本到语音转换程序无法正确处理内存中的对象时，可能就会触发该漏洞。成功利用漏洞的攻击者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、或者创建新帐户等。

8、Chakra 脚本引擎安全漏洞（CNNVD-201812-450、CVE-2018-8629）、（CNNVD-201812-455、CVE-2018-8624）、（CNNVD-201812-459、CVE-2018-8618 ）、（CNNVD-201812-460 、CVE-2018-8617）、（CNNVD-201812-470、CVE-2018-8583）

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。

9、Windows 权限提升漏洞（CNNVD-201812-442、CVE-2018-8641）、（CNNVD-201812-443、CVE-2018-8639）、（CNNVD-201812-462、CVE-2018-8611）

漏洞简介：当 Windows 内核无法正确处理内存中的对象时，可能就会触发该漏洞。攻击者首先必须登录到系统。然后运行一个经特殊设计的应用程序，才能利用此漏洞。成功利用漏洞的攻击者可以在内核模式中运行任意代码。攻击者可任意安装程序、查看、更改或删除数据、或者创建新帐户等。

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，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	Internet Explorer 安全漏洞（CNNVD-201812-458、CVE-2018-8619）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8619
2	Microsoft Outlook 安全漏洞（CNNVD-201812-469 、CVE-2018-8587）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8587

3	Microsoft Excel 安全漏洞（CNNVD-201812-466、CVE-2018-8597 ）、（ CNNVD-201812-446 、CVE-2018-8636）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8597 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8636
4	Microsoft PowerPoint 安全漏洞（CNNVD-201812-451 、CVE-2018-8628）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8628
5	Microsoft VBScript 安全漏洞（CNNVD-201812-454 、CVE-2018-8625）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8625
6	Microsoft.NET Framework 安全漏洞（CNNVD-201812-472 、CVE-2018-8540）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8540
7	Microsoft 文本到语音转换程序安全漏洞（CNNVD-201812-448 、CVE-2018-8634）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8634

8	Chakra 脚本引擎安全漏洞（CNNVD-201812-450 、CVE-2018-8629） 、（CNNVD-201812-455 、CVE-2018-8624）、（CNNVD-201812-459 、CVE-2018-8618）（ CNNVD-201812-460 、CVE-2018-8617） 、（CNNVD-201812-470 、CVE-2018-8583）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8617 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8618 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8624 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8629 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8583
9	Windows 权限提升漏洞（CNNVD-201812-442 、CVE-2018-8641） 、（CNNVD-201812-443 、CVE-2018-8639） 、（CNNVD-201812-462 、CVE-2018-8611）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8641 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8639 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8611