国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2018 年 10 月 15 日-2018 年 10 月 21 日 **2018 年第 42 期**

本周漏洞态势研判情况

本周信息安全漏洞威胁整体评价级别为**中**。

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 244 个，其中高危漏洞 101 个、中危漏洞 130 个、低危漏洞 13 个。漏洞平均分值为 6.36。本周收录的漏洞中，涉及 0day 漏洞 75 个（占 31%），其中互联网上出现“WAGO 750-881 Ethernet Controller 设备跨站脚本漏洞、WordPress 插件 tajer 任意文件上传漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 739 个，与上周（679 个）环比增长 9%。

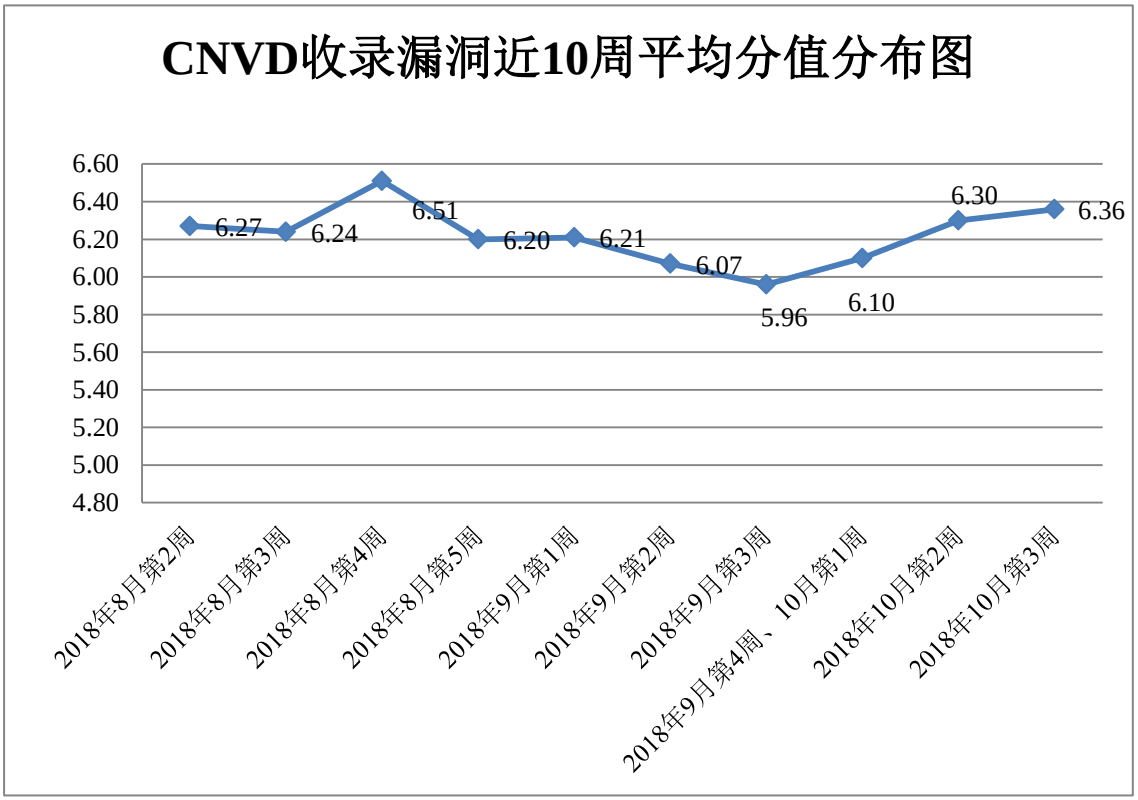

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞事件处置情况

本周，CNVD 向基础电信企业通报漏洞事件 5 起，向银行、证券、保险、能源等重要行业单位通报漏洞事件 24 起，协调 CNCERT 各分中心验证和处置涉及地方重要部门漏洞事件 204 起，协调教育行业应急组织验证和处置高校科研院所系统漏洞事件 34 起，向国家上级信息安全协调机构上报涉及部委门户、子站或直属单位信息系统漏洞事件 20 起。

此外，CNVD 通过已建立的联系机制或涉事单位公开联系渠道向以下单位通报了其信息系统或软硬件产品存在的漏洞，具体处置单位情况如下所示：

成都龙兵科技有限公司、金山软件股份有限公司、长沙德尚网络科技有限公司、天津国智恒北斗科技有限公司、北京费尔之盾科技有限公司、成都康菲顿特网络科技有限公司、沧州市凡诺广告传媒有限公司、杭州雄迈信息技术有限公司、上海亿速网络科技有限公司、淄博闪灵网络科技有限公司、中船重工鹏力（南京）智能装备系统有限公司、长沙翱云网络科技有限公司、中国新闻出版传媒集团有限公司、用友软件股份有限公司、中国中药有限公司、北京科维能动信息技术有限公司、中华税务信息网、中国财经网、IMA 中国教育分会、中国电子学会、科龙伟特 CMS、老班 cms、先进制造技术研究所研究生管理办公室、12321 网络不良与垃圾信息举报受理中心、PHPMyWind、扬子晚报、中国人民大学出版社、搜狗公司。

本周，CNVD 发布了《Oracle 发布 2018 年 10 月的安全公告》。详情参见 CNVD 网站公告内容。

http://www.cnvd.org.cn/webinfo/show/4717

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，新华三技术有限公司、蓝盾信息安全技术有限公司、哈尔滨安天科技股份有限公司、北京天融信网络安全技术有限公司、华为技术有限公司等单位报送公开收集的漏洞数量较多。山东云天安全技术有限公司、北京圣博润高新技术股份有限公司、任子行网络技术股份有限公司、远江盛邦（北京）网络安全科技股份有限公司、中新网络信息安全股份有限公司、河南信安世纪科技有限公司、山石网科通信技术有限公司、南京联成科技发展股份有限公司、北京明朝万达科技股份有限公司（安元实验室）、国家互联网应急中心研究所，北京同余科技有限公司及其他个人白帽子向 CNVD 提交了 739 个以事件型漏洞为主的原创漏洞，其中包括 360 网神（补天平台）和漏洞盒子向 CNVD 共享的白帽子报送的 408 条原创漏洞信息。

表 1 漏洞报送情况统计表

报送单位或个人	漏洞报送数量	原创漏洞数量

新华三技术有限公司	422	0
蓝盾信息安全技术有限公司	298	0
哈尔滨安天科技股份有限公司	220	0
漏洞盒子	216	216
北京天融信网络安全技术有限公司	206	11
华为技术有限公司	204	0
北京神州绿盟科技有限公司	193	0
360 网神（补天平台）	192	192
中国电信集团系统集成有限责任公司	144	0
北京数字观星科技有限公司	115	0
北京启明星辰信息安全技术有限公司	67	9
恒安嘉新(北京)科技股份公司	51	0
北京知道创宇信息技术有限公司	51	47
深圳市深信服电子科技有限公司	24	0
沈阳东软系统集成工程有限公司	6	6
北京无声信息技术有限公司	7	0
山东云天安全技术有限公司	93	93
北京圣博润高新技术股份有限公司	22	22
任子行网络技术股份有限公司	17	17
远江盛邦（北京）网络安全科技股份有限公司	10	10
中新网络信息安全股份有限公司	7	7
河南信安世纪科技有限公司	6	6

山石网科通信技术有限公司	3	3
南京联成科技发展股份有限公司	2	2
北京明朝万达科技股份有限公司（安元实验室）	1	1
国家互联网应急中心研究所，北京同余科技有限公司	1	1
CNCERT 上海分中心	9	9
CNCERT 贵州分中心	6	6
CNCERT 湖南分中心	4	4
CNCERT 吉林分中心	1	1
CNCERT 广东分中心	1	1
个人	75	75
报送总计	2674	739

本周漏洞按类型和厂商统计

本周，CNVD 收录了 244 个漏洞。应用程序漏洞 138 个，网络设备漏洞 39 个，WEB 应用漏洞 36 个，操作系统漏洞 27 个，安全产品漏洞 2 个，数据库漏洞 2 个。

表 2 漏洞按影响类型统计表

漏洞影响对象类型	漏洞数量
应用程序漏洞	138
网络设备漏洞	39
WEB 应用漏洞	36
操作系统漏洞	27
安全产品漏洞	2
数据库漏洞	2

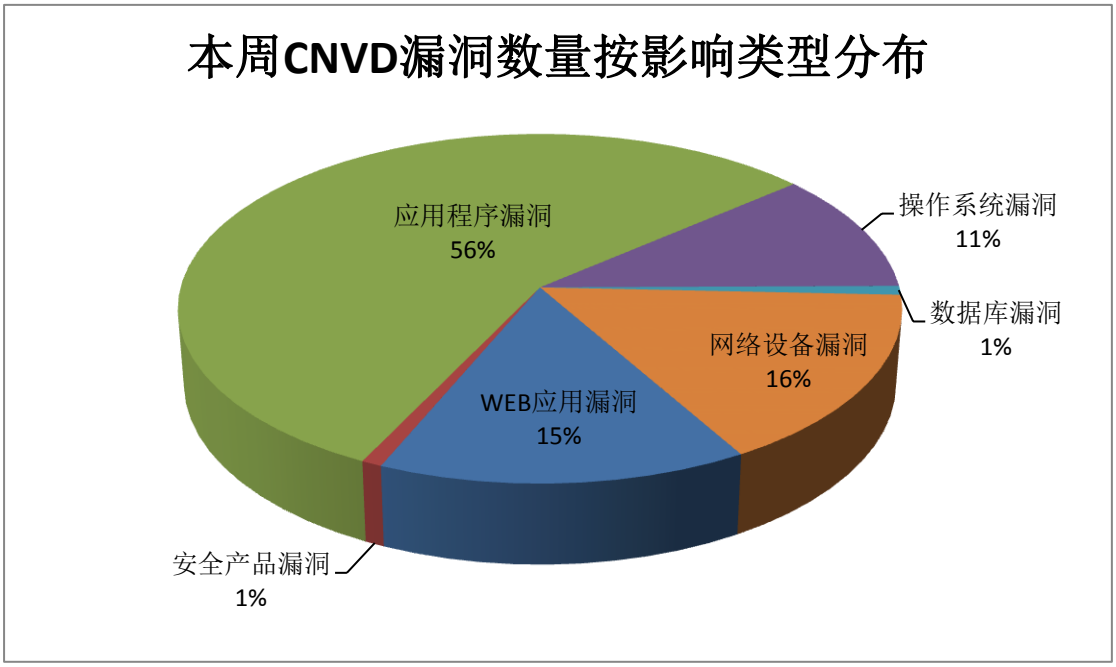

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Microsoft、Cisco、Adobe 等多家厂商的产品，部分漏洞数量按厂商统计如表 3 所示。

表 3 漏洞产品涉及厂商分布统计表

序号	厂商（产品）	漏洞数量	所占比例
1	Microsoft	25	10%
2	Cisco	19	8%
3	Adobe	18	7%
4	Apple	15	6%
5	Oracle	10	4%
6	WordPress	10	4%
7	Joomla!	7	3%
8	F5	6	3%
9	IBM	6	3%
10	其他	128	52%

本周行业漏洞收录情况

本周，CNVD 收录了 30 个电信行业漏洞，17 个移动互联网行业漏洞，17 个工控行业漏洞（如下图所示）。其中，“D-Link 路由器 httpd server 目录遍历漏洞、Cisco SD-WAN 证书验证安全绕过漏洞、多款 Apple 产品 WebKit 内存错误引用漏洞（CNVD-2018-20996）、

NUUO CMS 权限提升漏洞、LAquis SCADA 越界读取漏洞”等漏洞的综合评级为“高危”。相关厂商已经发布了上述漏洞的修补程序，请参照 CNVD 相关行业漏洞库链接。

电信行业漏洞链接：http://telecom.cnvd.org.cn/

移动互联网行业漏洞链接：http://mi.cnvd.org.cn/

工控系统行业漏洞链接：http://ics.cnvd.org.cn/

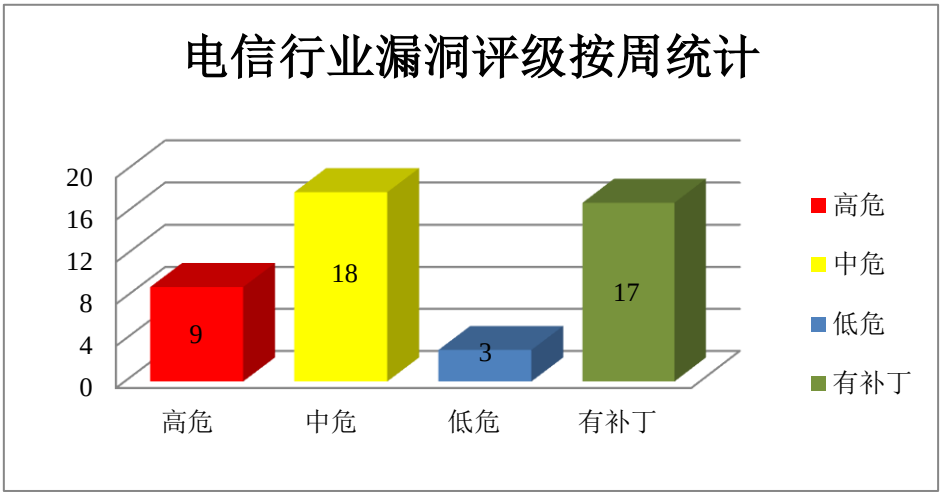

图 3 电信行业漏洞统计

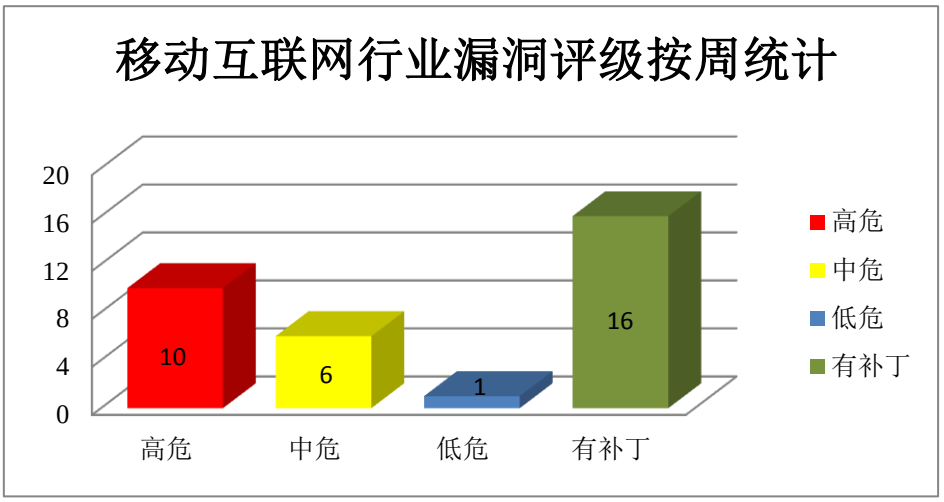

图 4 移动互联网行业漏洞统计

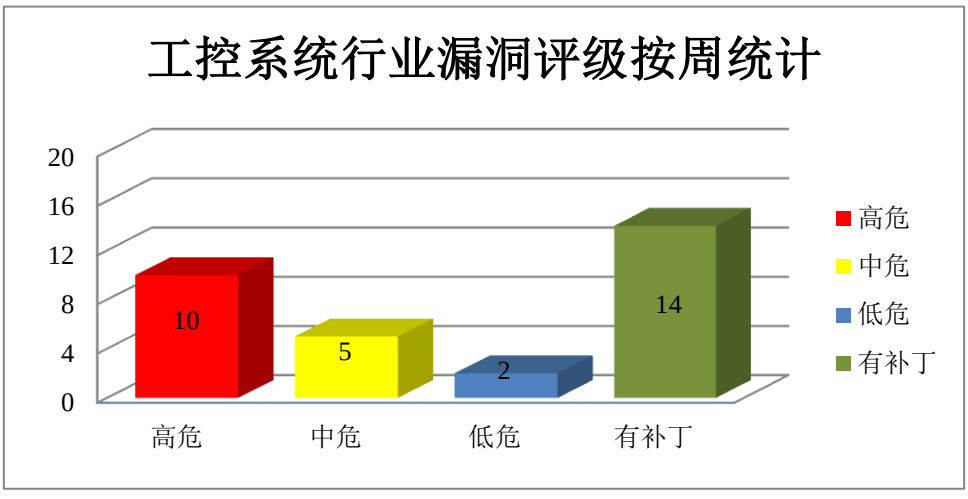

图 5 工控系统行业漏洞统计

本周重要漏洞安全告警

本周，CNVD 整理和发布以下重要安全漏洞信息。

1、Microsoft 产品安全漏洞

Microsoft C SDK for Azure IoT 是一款基于 C 语言的，用于开发 Azure IoT（物联网平台）应用程序的软件开发工具包。Edge 是微软操作系统附带的默认浏览器。ChakraCore 是使用在 Edge 中的一个开源的 JavaScript 引擎的核心部分，也可作为单独的 JavaScript 引擎使用。本周，上述产品被披露存在远程内存破坏漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft ChakraCore Scripting Engine 远程内存破坏漏洞（CNVD-2018-21212、CNVD-2018-21236）、Microsoft Edge Chakra Scripting Engine 远程内存破坏漏洞（CNVD-2018-21213、CNVD-2018-21216、CNVD-2018-21218、CNVD-2018-21219）、Microsoft Azure IoT Device Client SDK 远程内存破坏漏洞、Microsoft Edge Chakra Scripting Engine 远程内存破坏漏洞。上述漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2018-21212
http://www.cnvd.org.cn/flaw/show/CNVD-2018-21236
http://www.cnvd.org.cn/flaw/show/CNVD-2018-21213
http://www.cnvd.org.cn/flaw/show/CNVD-2018-21216
http://www.cnvd.org.cn/flaw/show/CNVD-2018-21218
http://www.cnvd.org.cn/flaw/show/CNVD-2018-21219
http://www.cnvd.org.cn/flaw/show/CNVD-2018-21220
http://www.cnvd.org.cn/flaw/show/CNVD-2018-21221

2、Cisco 产品安全漏洞

Cisco Wireless LAN Controller（WLC）是一款无线局域网控制器产品。Cisco Identity Services Engine（ISE）是一款基于身份的环境感知平台（ISE 身份服务引擎）。Cisco Webex Network Recording Player 和 Webex Player 都是用于播放视频会议记录的播放器。Cisco vEdge 100 Series Routers 等都是不同系列的路由器产品。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，绕过证书检测，提升权限，执行任意代码。

CNVD 收录的相关漏洞包括：Cisco Wireless LAN Controller Software GUI 权限提升漏洞、Cisco Wireless LAN Controller Software 目录遍历漏洞、Cisco Wireless LAN Controller Software Control and Provisioning of Wireless Access Points Protocol 信息

泄露漏洞、Cisco SD-WAN 证书验证安全绕过漏洞、Cisco Identity Services Engine WEB 管理接口任意命令执行漏洞（CNVD-2018-21257、CNVD-2018-21258）、Cisco Webex Network Recording Player 和 Webex Player 任意代码执行漏洞、Cisco Webex Network Recording Player 和 Webex Player 远程代码执行漏洞。上述漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2018-21192
http://www.cnvd.org.cn/flaw/show/CNVD-2018-21195
http://www.cnvd.org.cn/flaw/show/CNVD-2018-21194
http://www.cnvd.org.cn/flaw/show/CNVD-2018-21254
http://www.cnvd.org.cn/flaw/show/CNVD-2018-21257
http://www.cnvd.org.cn/flaw/show/CNVD-2018-21258
http://www.cnvd.org.cn/flaw/show/CNVD-2018-21328
http://www.cnvd.org.cn/flaw/show/CNVD-2018-21329

3、Adobe 产品安全漏洞

Adobe Acrobat 是一套 PDF 文件编辑和转换工具，Adobe Reader 是一套 PDF 文档阅读软件。本周，上述产品被披露存在任意代码执行漏洞，攻击者可利用漏洞执行任意代码（越界写入）。

CNVD 收录的相关漏洞包括：Adobe Acrobat 和 Reader 任意代码执行漏洞（CNVD-2018-21091、CNVD-2018-21092、CNVD-2018-21093、CNVD-2018-21094、CNVD-2018-21095、CNVD-2018-21096、CNVD-2018-21097、CNVD-2018-21098）。上述漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2018-21091
http://www.cnvd.org.cn/flaw/show/CNVD-2018-21092
http://www.cnvd.org.cn/flaw/show/CNVD-2018-21093
http://www.cnvd.org.cn/flaw/show/CNVD-2018-21094
http://www.cnvd.org.cn/flaw/show/CNVD-2018-21095
http://www.cnvd.org.cn/flaw/show/CNVD-2018-21096
http://www.cnvd.org.cn/flaw/show/CNVD-2018-21097
http://www.cnvd.org.cn/flaw/show/CNVD-2018-21098

4、Apple 产品安全漏洞

Apple iOS 是为移动设备所开发的一套操作系统；Safari 是一款 Web 浏览器，是 Mac OS X 和 iOS 操作系统附带的默认浏览器。iTunes for Windows 是一款基于 Windows 平台的媒体播放器应用程序。macOS Mojava 是一套专为 Mac 计算机所开发的专用操作系统；

tvOS 是一套智能电视操作系统；watchOS 是一套智能手表操作系统。本周，该产品被披露存在内存破坏和内存错误引用漏洞，攻击者可利用漏洞执行任意代码（内存破坏）。

CNVD 收录的相关漏洞包括：多款 Apple 产品 Kernel 内存破坏漏洞（CNVD-2018-20992）、多款 Apple 产品 WebKit 内存错误引用漏洞（CNVD-2018-20995、CNVD-2018-20996、CNVD-2018-20997、CNVD-2018-20998、CNVD-2018-20999、CNVD-2018-21000、CNVD-2018-21001）。上述漏洞的综合评级为“高危”。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2018-20992

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20995

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20996

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20997

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20998

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20999

http://www.cnvd.org.cn/flaw/show/CNVD-2018-21000

http://www.cnvd.org.cn/flaw/show/CNVD-2018-21001

5、Wecon PI Studio HMI 和 PI Studio 缓冲区溢出漏洞

Wecon PI Studio HMI 和 PI Studio 都是人机界面编程软件。。本周，Wecon PI Studio HMI 4.1.9 和 PI Studio 被披露存在缓冲区溢出漏洞。远程攻击者可利用该漏洞执行代码。CNVD 提醒广大用户随时关注厂商主页，以获取最新版本。参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2018-21172

更多高危漏洞如表 4 所示，详细信息可根据 CNVD 编号，在 CNVD 官网进行查询。参考链接：http://www.cnvd.org.cn/flaw/list.htm

表 4 部分重要高危漏洞列表

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2018-20872	TPEditor 栈缓冲区溢出漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：http://www.deltaww.com/Products/PluginWebUserControl/downloadCenterCounter.aspx?DID=4536&DocPath=1&hl=en-US
CNVD-2018-20874	Microsoft Windows Shell 远程执行代码漏洞（CNVD-2018-20874）	高	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-2018-8495
CNVD-2018-20876	Fastweb FASTGate modem 未授权远程命令执行漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：

			https://www.fastweb.it/myfastpage/assistenza/guide/FASTGate/
CNVD-2018-21066	VMware ESXi, Workstation and Fusion 越界读取漏洞	高	用户可联系供应商获得补丁信息：https://www.vmware.com/security/advisories/VMSA-2018-0026.html
CNVD-2018-21073	Dell EMC ESRS Virtual Edition 不正确的文件权限漏洞	高	用户可联系供应商获得补丁信息：https://www.dell.com/zh-cn
CNVD-2018-21087	Oracle WebLogic Server 远程代码执行漏洞（CNVD-2015-07707）	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html
CNVD-2018-21103	Bluetooth 安全绕过漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.bluetooth.com/news/unknown/2018/07/bluetooth-sig-security-update
CNVD-2018-21199	Libssh 服务器端身份验证绕过漏洞	高	用户可联系供应商获得补丁信息：https://www.libssh.org/2018/10/16/libssh-0-8-4-and-0-7-6-security-and-bugfix-release/
CNVD-2018-21247	Cloud Foundry CF Networking SQL 注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.cloudfoundry.org/blog/cve-2018-15755/
CNVD-2018-20866	strongSwan GMP 插件缓冲区溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.strongswan.org/blog/2018/10/01/strongswan-vulnerability-(cve-2018-17540).html

小结：本周，Microsoft 被披露存在远程内存破坏漏洞，攻击者可利用漏洞执行任意代码。此外，Cisco、Adobe、Apple 等多款产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，绕过证书检测，提升权限，执行任意代码（内存破坏）。另外，Wecon PI Studio HMI 和 PI Studio 被披露存在缓冲区溢出漏洞。远程攻击者可利用该漏洞执行代码。建议相关用户随时关注上述厂商主页，及时获取修复补丁或解决方案。

本周重要漏洞攻击验证情况

本周，CNVD 建议注意防范以下已公开漏洞攻击验证情况。

1、WAGO 750-881 Ethernet Controller 设备跨站脚本漏洞

验证描述

WAGO 750-881 Ethernet Controller devices 是德国 WAGO 公司的一款以太网控制器设备。

WAGO 750-881 Ethernet Controller 设备 01.09.18(13)及之前版本中的 webserv/cplcfg/snmp.ssi 文件的 SNMP 配置存在跨站脚本漏洞,远程攻击者可借助 SNMP_DESC 或 SNMP_LOC_SNMP_CONT 字段利用该漏洞注入任意的 Web 脚本或 HTML。

验证信息

POC 链接：https://www.exploit-db.com/exploits/45581/

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2018-21245

信息提供者

恒安嘉新(北京)科技股份公司

注：以上验证信息(方法)可能带有攻击性，仅供安全研究之用。请广大用户加强对漏洞的防范工作，尽快下载相关补丁。

本周漏洞要闻速递

1. Teltonika 路由器存在远程命令执行漏洞（CVE-2018-17532）

2018 年 10 月中旬， Teltonika 路由器存在远程命令执行漏洞。该漏洞是由于 RUT9XX 路由器设备中某些文件存在接受外部输入的参数，而这些参数在接收用户输入后，并未能检查其中是否有敏感字符，而是直接带入命令执行函数。攻击者只需要往存在漏洞的页面直接提交含有引号、分号等敏感字符的数据，就可使程序执行攻击者的命令，使这些路由设备变成肉鸡，成为僵尸网络中的一员，亦或者是挤占设备 CPU 进行挖矿，造成大量经济损失。

参考链接：https://www.anquanke.com/post/id/162187

2. WebLogic 远程代码执行漏洞（CVE-2018-3191）

北京时间 10 月 17 日，Oracle 官方发布的 10 月关键补丁更新 CPU（Critical Patch Update）中修复了一个高危的 WebLogic 远程代码执行漏洞（CVE-2018-3191）。该漏洞允许未经身份验证的攻击者通过 T3 协议网络访问并破坏易受攻击的 WebLogic Server，成功的漏洞利用可导致 WebLogic Server 被攻击者接管，从而造成远程代码执行。

参考链接：https://www.anquanke.com/post/id/162274

关于 CNVD

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库，致力于建立国家统一的信息安全漏洞收集、发布、验证、分析等应急处理体系。

关于 CNCERT

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称是 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，为非政府非盈利的网络安全技术中心，是我国网络安全应急体系的核心协调机构。

作为国家级应急中心，CNCERT 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82991537