国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2018 年 8 月 20 日-2018 年 8 月 26 日 **2018 年第 34 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 230 个，其中高危漏洞 75 个、中危漏洞 152 个、低危漏洞 3 个。漏洞平均分值为 6.51。本周收录的漏洞中，涉及 0day 漏洞 44 个（占 19%），其中互联网上出现“WordPress 插件 Chained Quiz SQL 注入漏洞、Hycus CMS 认证绕过漏洞”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 986 个，与上周（942 个）环比增长 5%。

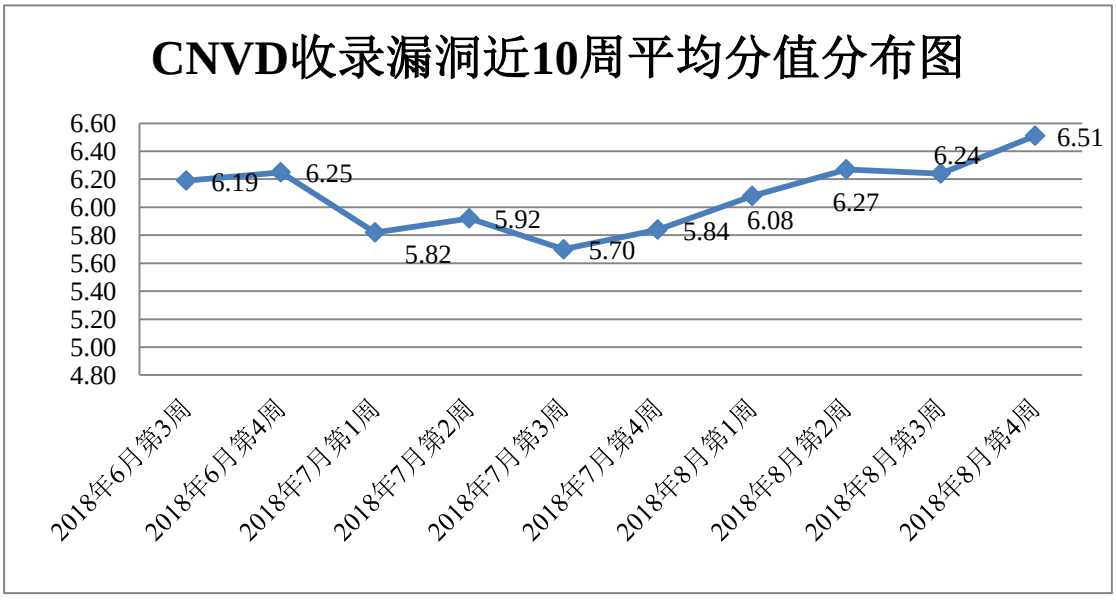

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京天融信网络安全技术有限公司、北京知道创宇信息技术有限公司、哈尔滨安天科技股份有限公司、北京数字观星科技有限公司、新

华三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、任子行网络技术股份有限公司、北京智游网安科技有限公司、南京联成科技发展股份有限公司、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、河北网信智安信息技术有限公司、山石网科通信技术有限公司、上海银基信息安全技术股份有限公司、四川虹微技术有限公司（子午攻防实验室）及其他个人白帽子向 CNVD 提交了 986 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 431 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
360 网神（补天平台）	308	308
北京天融信网络安全技术有限公司	292	18
北京知道创宇信息技术有限公司	280	272
哈尔滨安天科技股份有限公司	182	0
漏洞盒子	123	123
北京数字观星科技有限公司	122	0
新华三技术有限公司	101	0
北京神州绿盟科技有限公司	89	0
华为技术有限公司	79	0
中国电信集团系统集成有限责任公司	66	0
北京无声信息技术有限公司	29	27
恒安嘉新(北京)科技股份公司	25	0
深圳市深信服电子科技有限公司	19	0
西安四叶草信息技术有限公司	1	1
山东云天安全技术有限公司	39	39
任子行网络技术股份有限公司	22	22

北京智游网安科技有限公司	13	13
南京联成科技发展股份有限公司	12	12
中新网络信息安全股份有限公司	9	9
河南信安世纪科技有限公司	3	3
河北网信智安信息技术有限公司	2	2
山石网科通信技术有限公司	1	1
上海银基信息安全技术股份有限公司	1	1
四川虹微技术有限公司（子午攻防实验室）	1	1
CNCERT 黑龙江分中心	12	12
CNCERT 重庆分中心	7	7
CNCERT 上海分中心	6	6
CNCERT 湖南分中心	6	6
CNCERT 贵州分中心	4	4
CNCERT 吉林分中心	4	4
CNCERT 天津分中心	4	4
CNCERT 新疆分中心	2	2
个人	89	89
报送总计	1953	986

本周漏洞按类型和厂商统计

本周，CNVD 收录了 230 个漏洞。应用程序漏洞 162 个，网络设备漏洞 30 个，WEB 应用漏洞 19 个，操作系统漏洞 14 个，安全产品漏洞 3 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	162

网络设备漏洞	30
WEB 应用漏洞	19
操作系统漏洞	14
安全产品漏洞	3
数据库漏洞	2

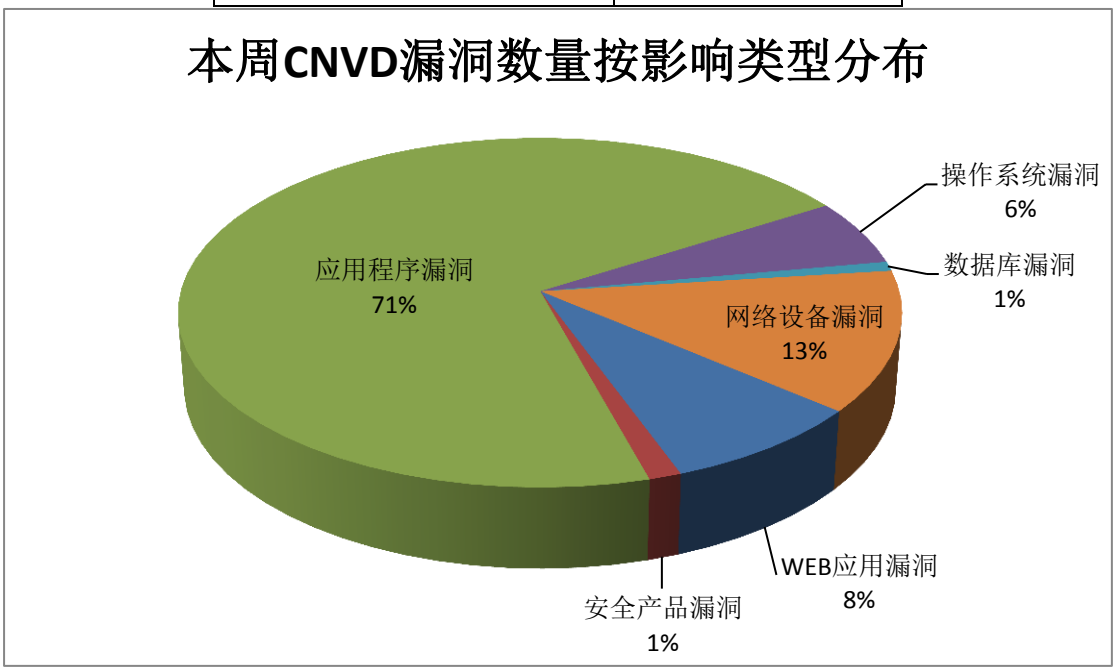

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Quest、Cisco、Microsoft 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	Quest	57	24%
2	Cisco	22	10%
3	Microsoft	19	8%
4	Google	9	4%
5	F5	6	3%
6	WordPress	6	3%
7	Adobe	5	2%
8	SAP	5	2%
9	Emerson Electric	4	2%
10	其他	97	42%

本周行业漏洞收录情况

本周，CNVD 收录了 10 个电信行业漏洞，12 个移动互联网行业漏洞，11 个工控行业漏洞（如下图所示）。其中，“PLANEX CS-W50HD 默认用户名密码漏洞、Emerson Electric DeltaV 栈缓冲区溢出漏洞、多款 Philips 产品硬编码凭证漏洞、Google Android Qualcomm 组件权限提升漏洞（CNVD-2018-16194）、Microsoft .NET Framework 远程代码执行漏洞（CNVD-2018-15850）”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/

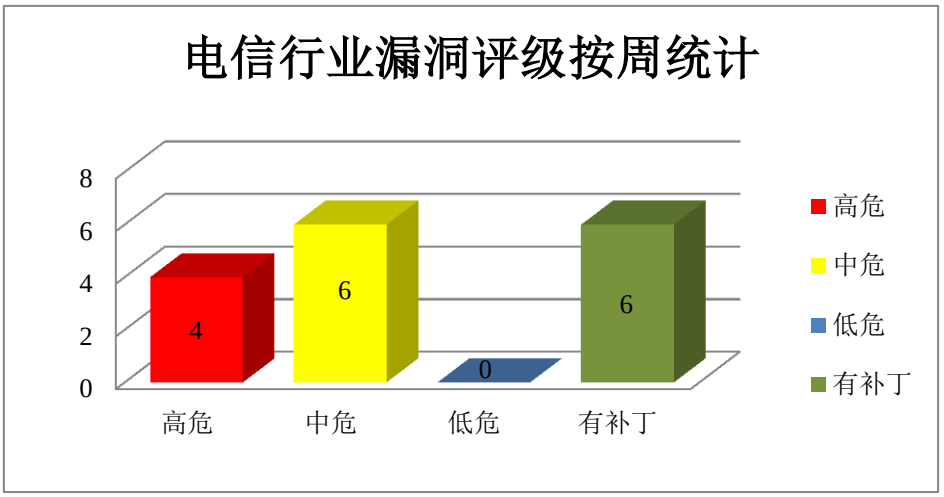

图 3 电信行业漏洞统计

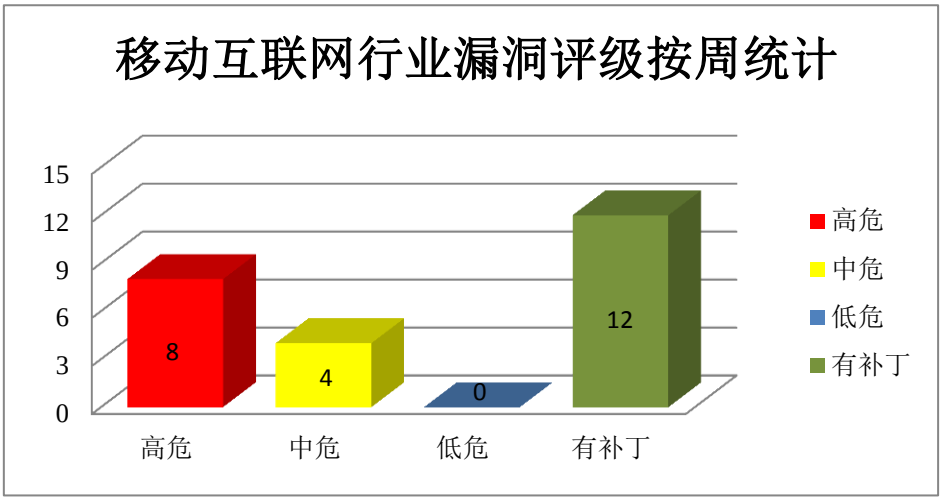

图 4 移动互联网行业漏洞统计

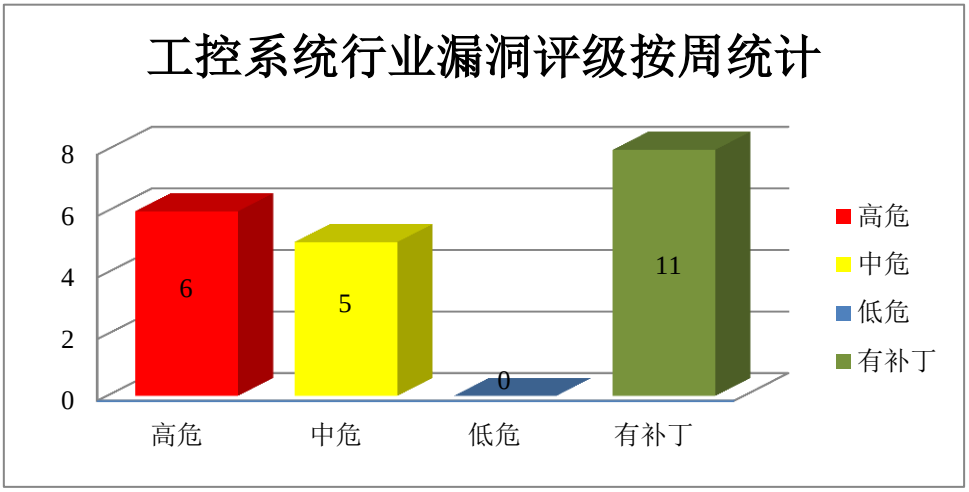

图 5 工控系统行业漏洞统计

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、Cisco 产品安全漏洞

Cisco Firepower System 是 Cisco Firepower 下一代防火墙使用的系统。Cisco Policy Suite 是电信级策略、收费及用户数据管理解决方案。Cisco IP Phone 6800、7800 和 8800 Series 都不同系列的 IP 电话产品。Multiplatform Firmware 是运行在其中的一套支持多平台的防火墙软件。Cisco FireSIGHT System 是一套集成的网络安全和流量管理产品，可部署在专用平台上或可作为软件解决方案。Cisco Web Security Appliance（WSA）是一套 Web 安全设备。Cisco DNA Center 是一个完整的基于软件的网络自动化和保障解决方案。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制，提升权限，执行任意代码。

CNVD 收录的相关漏洞包括：Cisco Policy Suite Policy Builder 认证绕过漏洞、Cisco Policy Suite Policy Builder 访问绕过漏洞、Cisco Firepower System 拒绝服务漏洞（CNVD-2018-16067）、Cisco IP Phone 6800、7800、8800 系列命令注入漏洞、Cisco FireSIGHT System 远程安全绕过漏洞、Cisco FireSIGHT System 远程安全绕过漏洞（CNVD-2018-16069）、Cisco Web Security Appliance 权限提升漏洞（CNVD-2018-16179）、Cisco Digital Network Architecture (DNA) Center 命令注入漏洞。其中，“Cisco IP Phone 6800、7800、8800 系列命令注入漏洞、Cisco Web Security Appliance 权限提升漏洞（CNVD-2018-16179）、Cisco Digital Network Architecture (DNA) Center 命令注入漏洞”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-2018-16064

http://www.cnvd.org.cn/flaw/show/CNVD-2018-16063

http://www.cnvd.org.cn/flaw/show/CNVD-2018-16067

http://www.cnvd.org.cn/flaw/show/CNVD-2018-16066

http://www.cnvd.org.cn/flaw/show/CNVD-2018-16068

http://www.cnvd.org.cn/flaw/show/CNVD-2018-16069

http://www.cnvd.org.cn/flaw/show/CNVD-2018-16179

http://www.cnvd.org.cn/flaw/show/CNVD-2018-16182

2、Microsoft 产品安全漏洞

Microsoft .NET Framework 是一种全面且一致的编程模型，也是一个用于构建 Windows、Windows Store、Windows Phone、Windows Server 和 Microsoft Azure 的应用程序的开发平台。该平台包括 C#和 Visual Basic 编程语言、公共语言运行库和广泛的类库。Microsoft ChakraCore 是一个 Edge（Web 浏览器）所使用的 JavaScript 引擎的核心部分。Internet Explorer 是一款网页浏览器。原称 Microsoft Internet Explorer(6 版本以前)和 Windows Internet Explorer(7、8、9、10、11 版本)，简称 IE。Edge 是微软为 Windows 10 打造的浏览器。Microsoft Windows 10 等都是操作系统。Edge 和 Internet Explorer（IE）都是其中的浏览器。前者是最新操作系统 Windows 10 附带的默认浏览器，后者是 Windows 10 之前操作系统附带的默认浏览器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获提升权限，执行任意代码，破坏内存。

CNVD 收录的相关漏洞包括：Microsoft .NET Framework 远程代码执行漏洞（CNVD-2018-15849、CNVD-2018-15850）、Microsoft ChakraCore 远程代码执行漏洞（CNVD-2018-15861、CNVD-2018-15862）、Microsoft Internet Explorer 和 Edge 脚本引擎内存破坏漏洞（CNVD-2018-15916、CNVD-2018-16174、CNVD-2018-16175）、Microsoft Internet Explorer 和 Edge 权限提升漏洞（CNVD-2018-15915）。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-2018-15849

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15850

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15861

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15862

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15916

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15915

http://www.cnvd.org.cn/flaw/show/CNVD-2018-16174

http://www.cnvd.org.cn/flaw/show/CNVD-2018-16175

3、Google 产品安全漏洞

安卓（Android）是一种基于 Linux 的自由及开放源代码的操作系统，由谷歌公司和开放手机联盟领导及开发。Google Chromium 是一款 Web 浏览器。Electron 是使用在其

中的一个使用 JavaScript、HTML 和 CSS 等 Web 技术创建桌面应用程序的框架。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，提升权限，执行任意代码。

CNVD 收录的相关漏洞包括：Google Android Qualcomm 组件权限提升漏洞（CNVD-2018-16191、CNVD-2018-16190）、Google Chromium Electron 远程代码执行漏洞、Google Android Qualcomm 组件权限提升漏洞（CNVD-2018-16194、CNVD-2018-16193）、Google Android Qualcomm 组件远程代码执行漏洞（CNVD-2018-16192）、Google Android System 信息泄露漏洞（CNVD-2018-16197）、Google Android Qualcomm 组件信息泄露漏洞（CNVD-2018-16195）。其中，除“Google Android System 信息泄露漏洞（CNVD-2018-16197）、Google Android Qualcomm 组件信息泄露漏洞（CNVD-2018-16195）”外，其余漏洞的综合评级为“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-2018-16191

http://www.cnvd.org.cn/flaw/show/CNVD-2018-16190

http://www.cnvd.org.cn/flaw/show/CNVD-2018-16189

http://www.cnvd.org.cn/flaw/show/CNVD-2018-16194

http://www.cnvd.org.cn/flaw/show/CNVD-2018-16193

http://www.cnvd.org.cn/flaw/show/CNVD-2018-16192

http://www.cnvd.org.cn/flaw/show/CNVD-2018-16197

http://www.cnvd.org.cn/flaw/show/CNVD-2018-16195

4、Quest 产品安全漏洞

Quest DR 系列是磁盘存储和重复数据删除设备。本周，该产品被披露存在权限提升和命令注入漏洞，攻击者可利用漏洞提升权限，执行任意代码。

CNVD 收录的相关漏洞包括：Quest DR 系列磁盘备份软件命令注入漏洞（CNVD-2018-15622、CNVD-2018-15865）、Quest DR 系列磁盘备份软件权限提升漏洞（CNVD-2018-15897、CNVD-2018-15903、CNVD-2018-15910、CNVD-2018-15909、CNVD-2018-15912、CNVD-2018-15911）。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-2018-15622

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15865

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15897

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15903

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15910

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15909

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15912

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15911

5、GhostScript 沙箱绕过(命令执行)漏洞

GhostScript 是 PostScript 和可移植文档格式（PDF）文件的解释器。本周，GhostScript 被披露存在沙箱绕过(命令执行)漏洞。攻击者可以利用该漏洞造成命令执行。目前，厂商尚未发布漏洞修补程序。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-2018-15995

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-2018-15731	Tridium Niagara AX Framework 和 Niagara 4 Framework 路径遍历漏洞	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.tridium.com/~/media/tridium/library/documents/niagara%20ax%2038%20update%204niagara%2044%20update%201.ashx?la=en
CNVD-2018-15734	多款 Philips 产品硬编码凭证漏洞	高	用户可联系供应商获得补丁信息：http://www.philips.com/productsecurity
CNVD-2018-15764	Zoho ManageEngine ADAudit Plus SQL 注入漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.manageengine.com/products/active-directory-audit/adaudit-plus-release-notes.html
CNVD-2018-15838	D-Link EyeOn Baby Monitor DCS-825L 堆栈溢出远程代码执行漏洞	高	用户可联系供应商获得补丁信息：http://www.dlink.com/
CNVD-2018-15840	PLANEX CS-QR20 任意代码执行漏洞	高	用户可联系供应商获得补丁信息：http://www.planex.co.jp/
CNVD-2018-15839	PLANEX CS-QR20 硬编码凭证漏洞	高	用户可联系供应商获得补丁信息：http://www.planex.co.jp/
CNVD-2018-15894	Apache Struts2 S2-057 远程代码执行漏洞	高	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞：https://cwiki.apache.org/confluence/display/WW/S2-057?tdsourcetag=s_pcqq_aiomsg
CNVD-2018-15895	Intel Distribution for Python Bleach 模块拒绝服务漏洞	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.intel.com/content/www/us/en/security-center/advisory/intel-sa-001

			29.html
CNVD-2018-15898	McAfee Drive Encryption TPM autoboot 身份认证绕过漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://kc.mcafee.com/corporate/index?page=content&id;=SB10242
CNVD-2018-15917	HPE Intelligent Management Center 任意代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.hpe.com/hpsc/doc/public/display?docId=hpesbhf03852en_us

小结：本周，Cisco 被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制，提升权限，执行任意代码。此外，Microsoft、Google、Quest 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，提升权限，执行任意代码，破坏内存等。另外，GhostScript 被披露存在沙箱绕过(命令执行)漏洞。攻击者可以利用该漏洞造成命令执行。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、WordPress 插件 Chained Quiz SQL 注入漏洞

验证描述

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。

WordPress 插件 Chained Quiz 存在 SQL 注入漏洞，攻击者可利用漏洞执行任意 SQL 命令。

验证信息

POC 链接：https://www.exploitalert.com/view-details.html?id=30666

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2018-15997

信息提供者

CNVD 工作组

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. 微软 VBScirpt 引擎中的 0day 漏洞遭 Darkhotel APT 利用

VBScript 可在 Windows 和 IE 11 最新版本上使用。不过微软在浏览器的默认设置中禁用了 Windows 最新版本中的 VBScript 执行，以解决该漏洞。尽管如此，但还存在加

载脚本的其它方法。例如，Office 组件中的应用依靠 IE 引擎加载并渲染 web 内容。

安全研究员早在微软于 7 月份交付 Windows 常规更新一天后就注意到这个 VBScript 漏洞遭利用。该漏洞的 CVE 编号是 CVE-2018-8373，已在本月的补丁日修复。它是一个使用后释放内存破坏漏洞，能让攻击者在受攻陷计算机上运行 shellcode。

参考链接：https://www.bleepingcomputer.com/news/security/zero-day-in-microsofts-vbscript-engine-used-by-darkhotel-apt/

2. 关于 Ghostscript SAFER 沙箱绕过漏洞的分析

Ghostscript 是一款 Adobe PostScript 语言的解释器软件。近日，Google 安全研究员披露了多个 GhostScript 的漏洞，通过在图片中构造恶意 PostScript 脚本，可以绕过 SAFER 安全沙箱，从而造成命令执行、文件读取、文件删除等漏洞，其根本原因是 GhostScript 解析 restore 命令时，会暂时关闭 SAFER。

参考链接：http://www.freebuf.com/column/182083.html

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