国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2017 年 03 月 27 日-2017 年 04 月 02 日 **2017 年第 14 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 396 个，其中高危漏洞 146 个、中危漏洞 216 个、低危漏洞 34 个。漏洞平均分值为 5.93。本周收录的漏洞中，涉及 0day 漏洞 81 个（占 20%），其中互联网上出现“Microsoft Windows Server 2003 R2 IIS 缓冲区溢出漏洞、Joomla! jCart For OpenCart 组件 SQL 注入漏洞”等零日代码攻击漏洞。此外，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 1119 个，与上周（624 个）相比增加 1.8 倍。

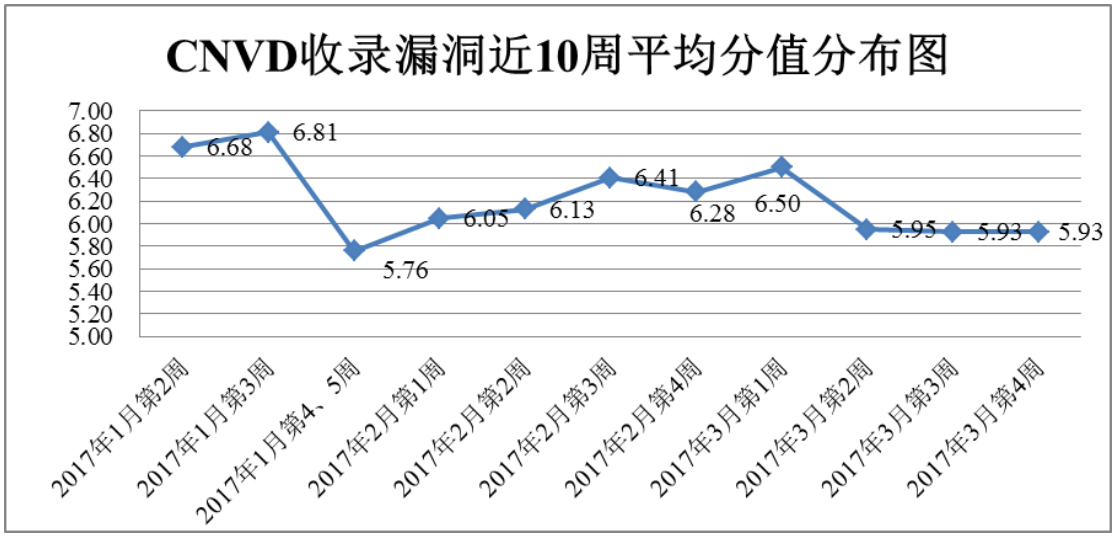

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周，共 17 家成员单位、合作伙伴及企业用户、个人用户报送了本周收录的全部 396 个漏洞。报送情况如表 1 所示。其中，蓝盾信息安全技术有限公司、安天实验室、启明星辰、华为技术有限公司、天融信等单位报送数量较多。漏洞盒子、安徽新华博信息技术股份有限公司、江西安服信息产业有限公司、河北网信智安信息技术有限公司、广

州万方计算机科技有限公司、山东安云信息技术有限公司、广州神月信息安全技术有限公司、清远职业技术学院、上海零盾网络科技有限公司及其他个人白帽子向 CNVD 提交了 1119 个以事件型漏洞为主的原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
360 网神	525	525
蓝盾信息安全技术有限公司	245	0
安天实验室	176	0
启明星辰	121	28
华为技术有限公司	115	0
天融信	109	0
杭州安恒信息技术有限公司	58	0
H3C	57	1
绿盟科技	48	0
中国电信集团系统集成有限责任公司	45	0
阿里云计算有限公司	18	0
安全狗	15	0
北京数字观星科技有限公司	5	0
恒安嘉新	2	0
深圳市深信服电子科技有限公司	2	2
西安四叶草信息技术有限公司	1	1
深圳市腾讯计算机系统有限公司（玄武实验室）	1	1
漏洞盒子	417	417
安徽新华博信息技术股份有限公司	9	9

江西安服信息产业有限公司	7	7
河北网信智安信息技术有限公司	5	5
广州万方计算机科技有限公司	5	5
山东安云信息技术有限公司	3	3
广州神月信息安全技术有限公司	3	3
清远职业技术学院	2	2
上海零盾网络科技有限公司	1	1
CNCERT 重庆分中心	6	6
CNCERT 广东分中心	5	5
CNCERT 福建分中心	5	5
CNCERT 江西分中心	4	4
CNCERT 浙江分中心	4	4
CNCERT 湖南分中心	4	4
CNCERT 北京分中心	2	2
CNCERT 吉林分中心	2	2
CNCERT 内蒙古分中心	1	1
个人	76	76
报送总计	2104	1119
录入总计	396（去重）	1119

表 1 漏洞报送情况统计表

本周漏洞按类型和厂商统计

本周，CNVD 收录了 396 个漏洞。其中应用程序漏洞 187 个，操作系统漏洞 91 个，web 应用漏洞 90 个，网络设备漏洞 18 个，安全产品漏洞 9 个，数据库漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	187
操作系统漏洞	91
web 应用漏洞	90
网络设备漏洞	18
安全产品漏洞	9
数据库漏洞	1

表 2 漏洞按影响类型统计表

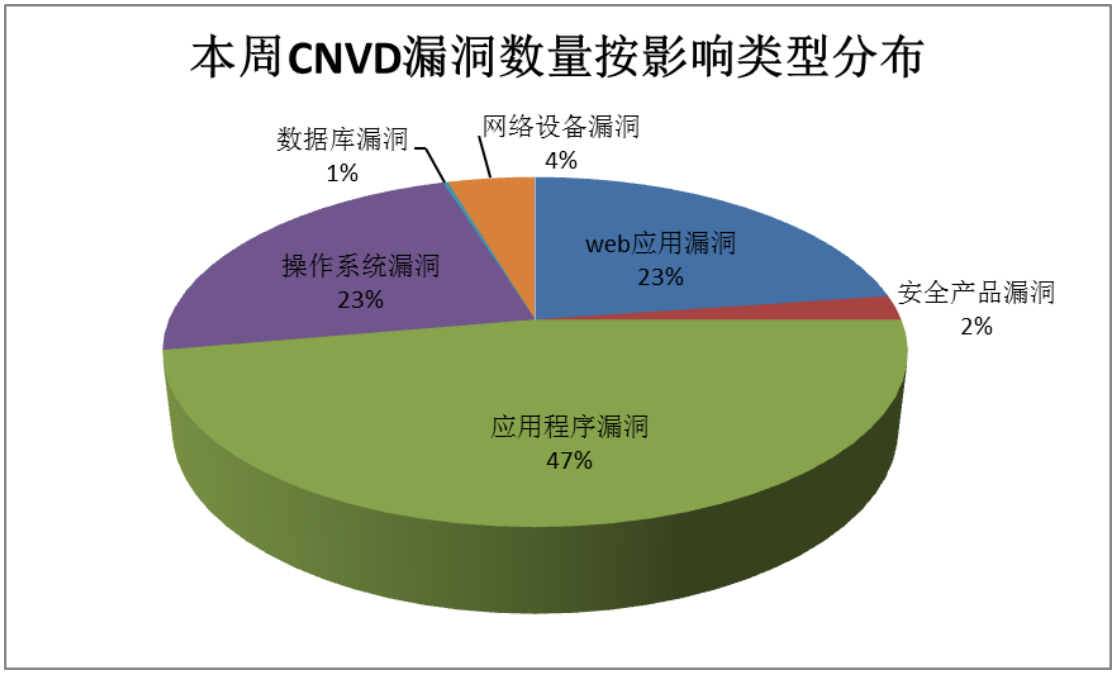

图 2 本周漏洞按影响类型分布

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

序号	厂商（产品）	漏洞数量	所占比例
1	Microsoft	102	26%
2	Google	39	10%
3	WordPress	20	5%
4	SAP	12	3%
5	Audio File Library	11	3%
6	Cisco	9	2%
7	IBM	6	2%
8	Fastspot	5	1%
9	Huawei	5	1%
10	其他	187	47%

表 3 漏洞产品涉及厂商分布统计表

本周行业漏洞收录情况

本周，CNVD 收录了 11 个电信行业漏洞，37 个移动互联网行业漏洞，1 个工控系统行业漏洞（如下图所示）。其中，“Android HTC Sensor Hub 驱动提权漏洞、Google Android MediaTek APK 权限提升漏洞、Android Qualcomm fingerprint sensor 驱动提权漏洞、Android kernel security 子系统提权漏洞、Android Qualcomm input hardware 驱动提权漏洞、Google Android Qualcomm IPA Driver 权限提升漏洞、Google Android NVIDIA GPU Driver 权限提升漏洞（CNVD-2017-03821、CNVD-2017-03836）”等的综合评级为“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/

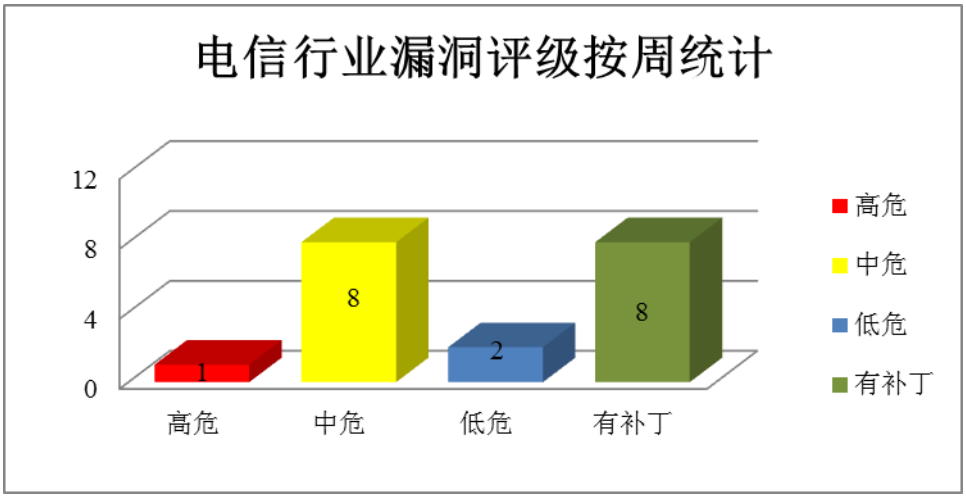

图 3 电信行业漏洞统计

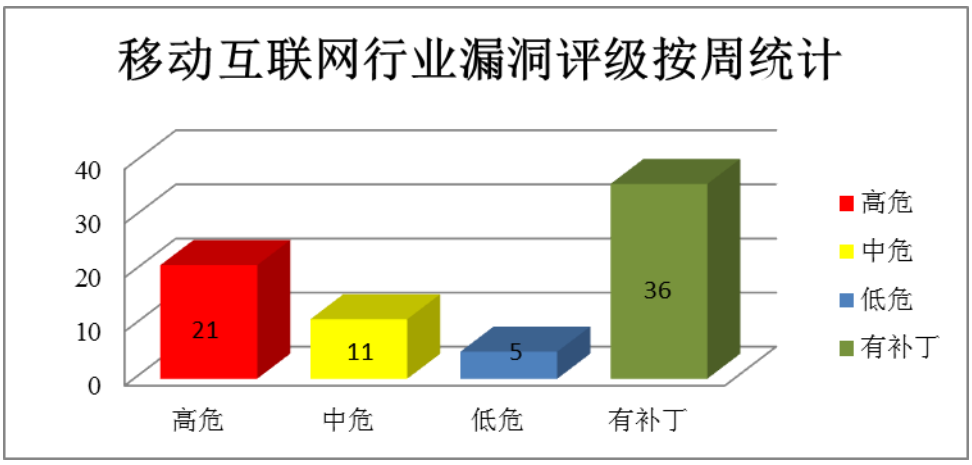

图 4 移动互联网行业漏洞统计

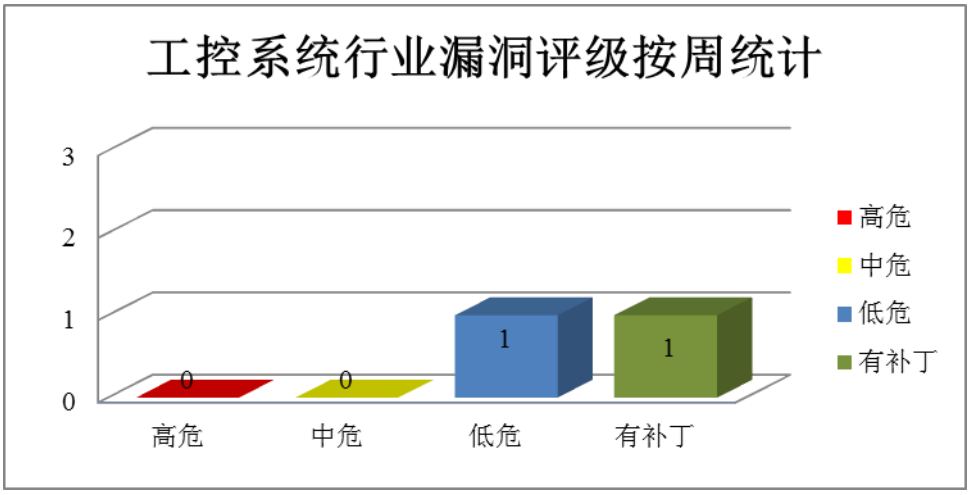

图 5 工控系统行业漏洞统计

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 Edge 是美国微软（Microsoft）公司开发的一款 Web 浏览器，是 Windows 10 操作系统附带的默认浏览器。Scripting Engine 是其中的一个 JavaScript 引擎组件。本周，上述产品被披露存在内存破坏漏洞，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 Edge 脚本引擎内存破坏漏洞（CNVD-2017-03366、CNVD-2017-03367、CNVD-2017-03368、CNVD-2017-03369、CNVD-2017-03370、CNVD-2017-03371、CNVD-2017-03372、CNVD-2017-03373）。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-2017-03366
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03367
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03368
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03369
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03370
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03371
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03372
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03373

2、Google 产品安全漏洞

Android 是美国谷歌公司和开放手持设备联盟共同开发的一套以 Linux 为基础的开源操作系统。MediaTek 是使用在其中的一个联发科（MediaTek）公司的设备专用的联发科组件。NVIDIA GPU Driver 是一个 NVIDIA 图形处理器驱动组件。本周，该产品

被披露存在权限提升漏洞，攻击者可利用漏洞提升权限。

CNVD 收录的相关漏洞包括：Google Android MediaTek 组件权限提升漏洞（CNVD-2017-03380、CNVD-2017-03381、CNVD-2017-03382、CNVD-2017-03383、CNVD-2017-03384、CNVD-2017-03385）、Google Android NVIDIA GPU Driver 权限提升漏洞（CNVD-2017-03821、CNVD-2017-03836）。上述的综合评级为“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-2017-03380
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03381
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03382
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03383
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03384
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03385
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03821
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03836

3、Cisco 产品安全漏洞

Cisco IOx 是美国思科（Cisco）公司的一套为思科物联网网络基础设施提供统一托管功能的应用程序。Cisco Adaptive Security Appliances Software 是一套运行于防火墙中的操作系统。Cisco TelePresence Server Software 是一套被称为“网真”系统的视频会议解决方案。Cisco NX-OS 是一个数据中心级的操作系统，Cisco Unified Communications Manager 是一款统一通信系统中的呼叫处理组件。Cisco WebEx Meetings Server 是 WebEx 会议方案中的一套包含音频、视频和 Web 会议的多功能会议解决方案。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、泄露敏感信息和发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Cisco Iox 任意文件修改漏洞、Cisco Adaptive Security Appliances Software 安全绕过漏洞、Cisco TelePresence Server Software 权限提升漏洞、Cisco NX-OS Software 拒绝服务漏洞（CNVD-2017-03769）、Cisco Unified Communications Manager 跨站脚本漏洞（CNVD-2017-03606）、Cisco Unified Computing System Director 跨站脚本漏洞、Cisco WebEx Meetings Server 认证绕过漏洞、Cisco WebEx Meetings Server XML 外部实体信息泄露漏洞。其中“Cisco WebEx Meetings Server XML 外部实体信息泄露漏洞”的综合评级为“高危”。目前，厂商已经发布了除“Cisco Unified Computing System Director 跨站脚本漏洞、Cisco WebEx Meetings Server 认证绕过漏洞、Cisco WebEx Meetings Server XML 外部实体信息泄露漏洞”外漏洞的修补程序。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-2017-03697

http://www.cnvd.org.cn/flaw/show/CNVD-2017-03544
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03767
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03769
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03606
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03770
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03768
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03607

4、SAP 产品安全漏洞

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。SAP NetWeaver 是一套面向服务的集成化应用平台。SAP ERP 是一套基于客户/服务机结构和开放系统的、集成的企业资源计划系统。SAP GUI 是图形用户界面客户端。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、远程执行任意代码或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：SAP ERP 远程授权绕过漏洞、SAP Netweaver Dynpro Engine 拒绝服务漏洞、SAP NetWeaver 存在未明安全绕过漏洞、SAP ERP 远程身份验证绕过漏洞、SAP GUI 远程代码执行漏洞、SAP HANA Extended Application Services SQL 注入漏洞、SAP HANA 拒绝服务漏洞（CNVD-2017-03576）、SAP HANA Web Workbench SQL 注入漏洞。其中，“SAP GUI 远程代码执行漏洞、SAP HANA Extended Application Services SQL 注入漏洞、SAP HANA 拒绝服务漏洞（CNVD-2017-03576）、SAP HANA Web Workbench SQL 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-2017-03492
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03498
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03497
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03496
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03495
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03494
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03576
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03499

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

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2017-03393	mcollective-puppet-agent 提升权限漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主

			页: https://puppet.com/security/cve/cve-2017-2290
CNVD-2017-03399	festivaltts4r gem for Ruby 远程命令执行漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页: https://github.com/spejman/festivaltts4r/issues/1
CNVD-2017-03448	GNU Binutils 拒绝服务漏洞	高	用户可联系供应商获得补丁信息：https://www.gnu.org/
CNVD-2017-03585	Apache NiFi 远程代码注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://seclists.org/oss-sec/2017/q1/565
CNVD-2017-03718	Huawei VCM5010 命令注入漏洞	高	华为已发布版本修复该漏洞，安全预警链接：http://www.huawei.com/cn/psirt/security-advisories/huawei-sa-20170329-01-vcm-cn
CNVD-2017-03717	Huawei VCM5010 任意文件上传漏洞	高	华为已发布版本修复该漏洞，安全预警链接：http://www.huawei.com/cn/psirt/security-advisories/huawei-sa-20170329-01-vcm-cn
CNVD-2017-03716	Huawei VCM5010 鉴权绕过漏洞	高	华为已发布版本修复该漏洞，安全预警链接：http://www.huawei.com/cn/psirt/security-advisories/huawei-sa-20170329-01-vcm-cn
CNVD-2017-03742	多款 VMware 产品内存破坏漏洞（CNVD-2017-03742）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.vmware.com/security/advisories/VMSA-2017-0005.html
CNVD-2017-03744	PoDoFo 缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://podofo.sourceforge.net/
CNVD-2017-03762	TeX Live 远程代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://scumjr.github.io/2016/11/28/pwning-coworkers-thanks-to-latex/

表 4 部分重要高危漏洞列表

小结：本周，Microsoft 被披露存在内存破坏漏洞，攻击者可利用漏洞执行任意代码。此外，Gooole、SAP、Cisco 等多款产品被披露存在多个漏洞，攻击者利用漏洞可执行任意代码、绕过安全限制、泄露敏感信息或发起拒绝服务攻击等。另外，Wonder 被披

露存在路径遍历漏洞，远程攻击者可借助特制的 theme 利用该漏洞读取任意文件。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。

本周漏洞要闻速递

1. IIS 6.0 曝远程代码执行漏洞 CVE-2017-7269

微软方面也已经确认了该漏洞：Windows Server 2003R2 版本 IIS6.0 的 WebDAV 服务中的 ScStoragePathFromUrl 函数存在缓存区溢出漏洞，远程攻击者通过以“If: <http://”开头的长 header PROPFIND 请求，执行任意代码。该漏洞自 2016 年 7、8 月起就已被利用。

参考链接：http://www.freebuf.com/vuls/130531.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：010-82990999