国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2018 年 1 月 8 日-2018 年 1 月 14 日 **2018 年第 2 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**高**。

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 257 个，其中高危漏洞 109 个、中危漏洞 134 个、低危漏洞 14 个。漏洞平均分值为 6.41。本周收录的漏洞中，涉及 0day 漏洞 78 个（占 30%），其中互联网上出现“Linksys WVBR0 无线网桥远程命令执行漏洞、Western Digital MyCloud PR4100 Web 管理组件'multi_uploadify'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 498 个，与上周（483 个）环比增长 3%。

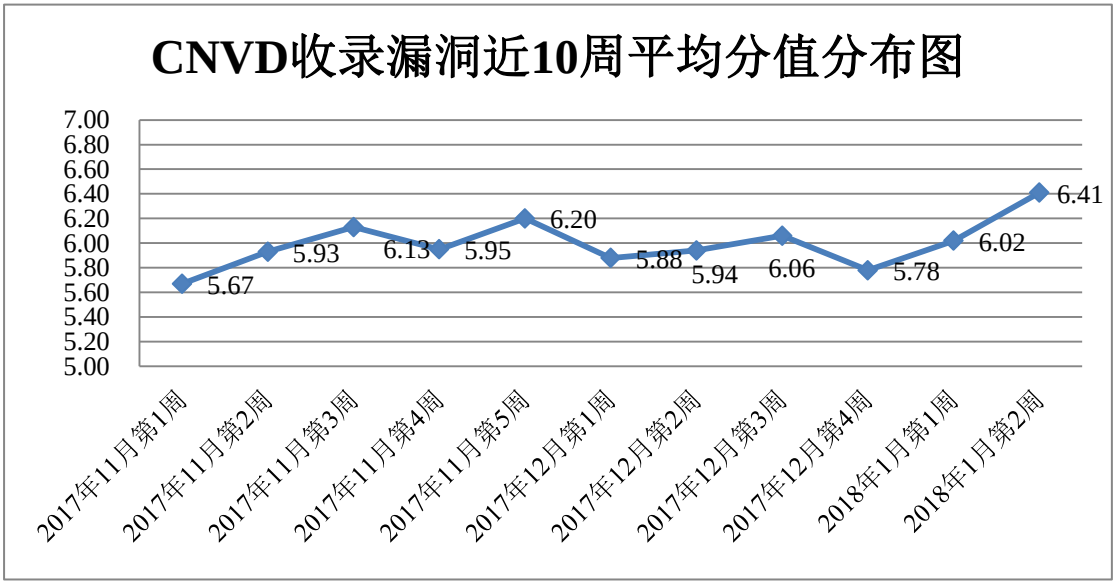

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，H3C、恒安嘉新、安天实验室、天融信、北京数字观星科技有限公司等单位报送数量较多。四川虹微技术有限公司（子午攻防实验室）、南京联成科技发展股份有限公司、福建省海峡信息技术有限公司、中新网络信息安全股

份有限公司、北京智游网安科技有限公司、邹平九零冰讯网络科技有限公司、博雅信安科技（北京）有限公司、成都思维世纪科技有限公司、漏斗社区及其他个人白帽子向 CNVD 提交了 498 个以事件型漏洞为主的原创漏洞。

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
H3C	252	0
恒安嘉新	233	0
安天实验室	218	0
360 网神	171	171
天融信	164	1
北京数字观星科技有限公司	90	0
中国电信集团系统集成有限责任公司	89	0
漏洞盒子	80	80
华为技术有限公司	62	0
绿盟科技	56	0
杭州安恒信息技术有限公司	55	0
卫士通信息产业股份有限公司	34	0
广西鑫瀚科技有限公司	3	3
知道创宇	2	0
四川虹微技术有限公司（子午攻防实验室）	21	21
南京联成科技发展股份有限公司	8	8
福建省海峡信息技术有限公司	7	7
中新网络信息安全股份有限公司	4	4
北京智游网安科技有限公司	2	2

邹平九零冰讯网络科技有限公司	1	1
博雅信安科技（北京）有限公司	1	1
成都思维世纪科技有限公司	1	1
漏斗社区	1	1
CNCERT 山西分中心	24	24
CNCERT 吉林分中心	6	6
CNCERT 上海分中心	5	5
CNCERT 河北分中心	4	4
CNCERT 福建分中心	2	2
CNCERT 新疆分中心	2	2
CNCERT 海南分中心	1	1
CNCERT 广东分中心	1	1
个人	152	152
报送总计	1752	498

本周漏洞按类型和厂商统计

本周，CNVD 收录了 257 个漏洞。其中应用程序漏洞 142 个，操作系统漏洞 63 个，web 应用漏洞 34 个，网络设备漏洞 11 个，安全产品漏洞 7 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	142
操作系统漏洞	63
web 应用漏洞	34
网络设备漏洞	11
安全产品漏洞	7

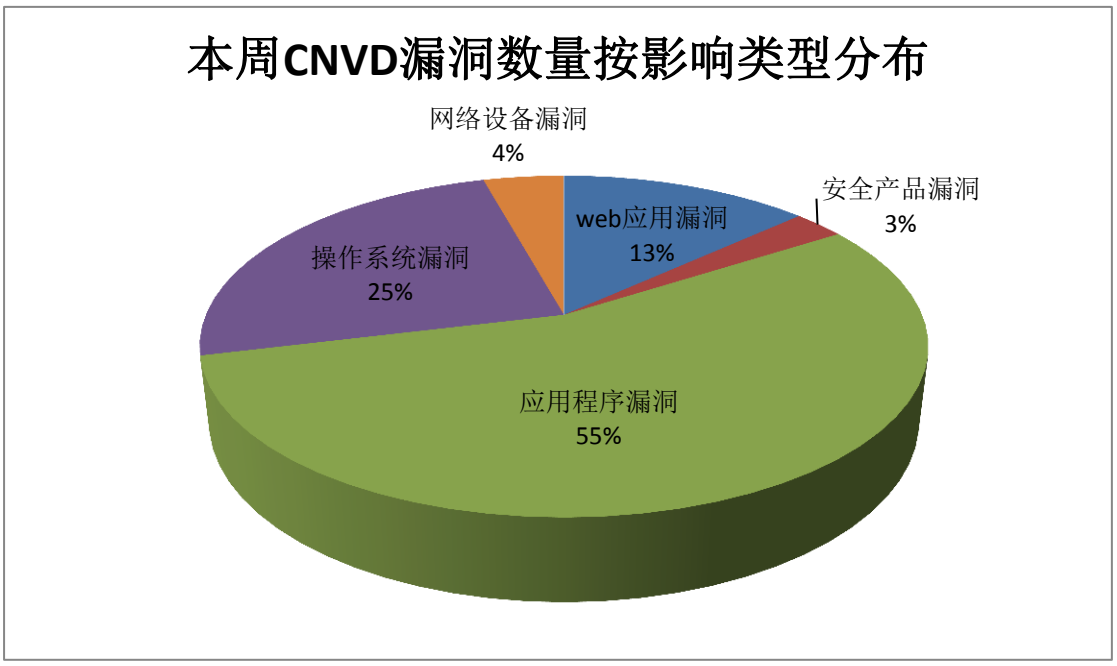

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Microsoft、Google、PHP Scripts Mall 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	58	23%
2	Google	27	11%
3	PHP Scripts Mall	19	7%
4	IBM	5	2%
5	Advantech	5	2%
6	Elemental Path's	3	1%
7	FiyoCMS	3	1%
8	Atlassian	3	1%
9	vBulletin	2	1%
10	其他	132	51%

本周行业漏洞收录情况

本周，CNVD 收录了 6 个电信行业漏洞，41 个移动互联网行业漏洞，6 个工控行业漏洞（如下图所示）。其中，“Advantech WebAccess 输入验证漏洞、Google Android Ashmem 组权限提升漏洞、Apple iOS 内存破坏漏洞（CNVD-2018-00598）、Google Andr

oid Runtime 权限提升漏洞、Google Qualcomm Bootloader 权限提升漏洞”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/

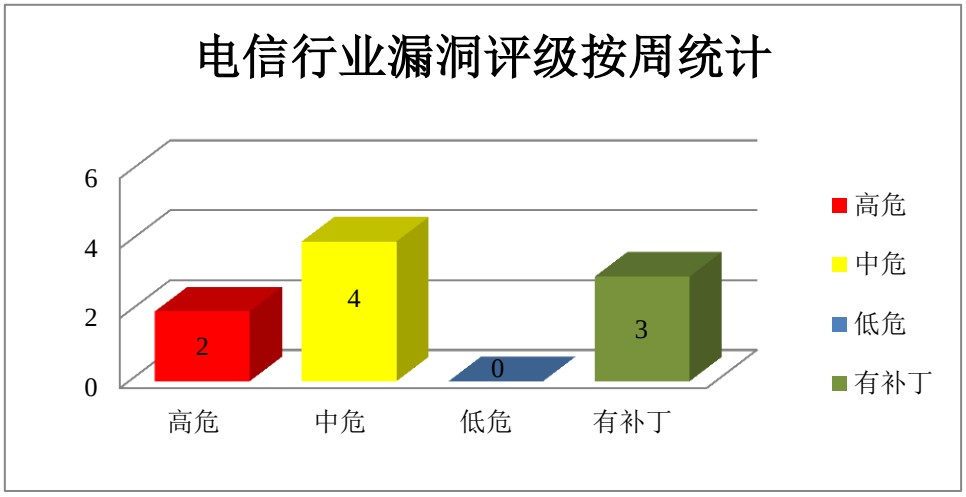

图 3 电信行业漏洞统计

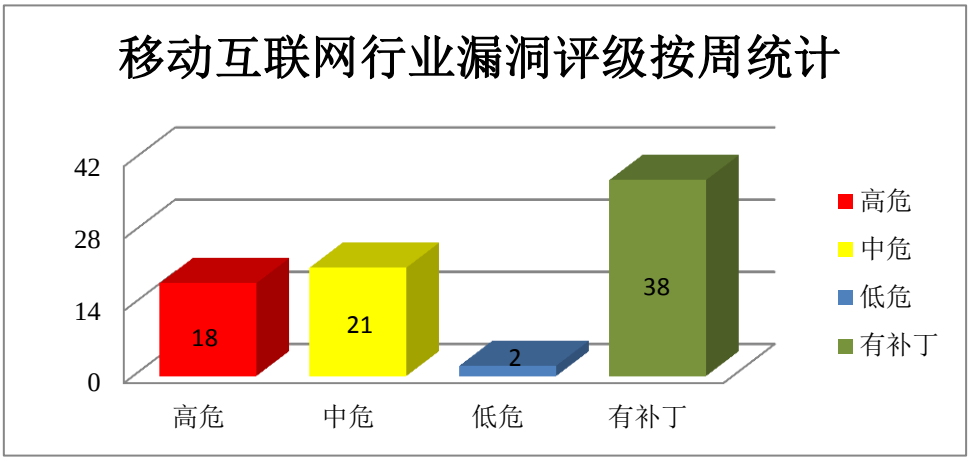

图 4 移动互联网行业漏洞统计

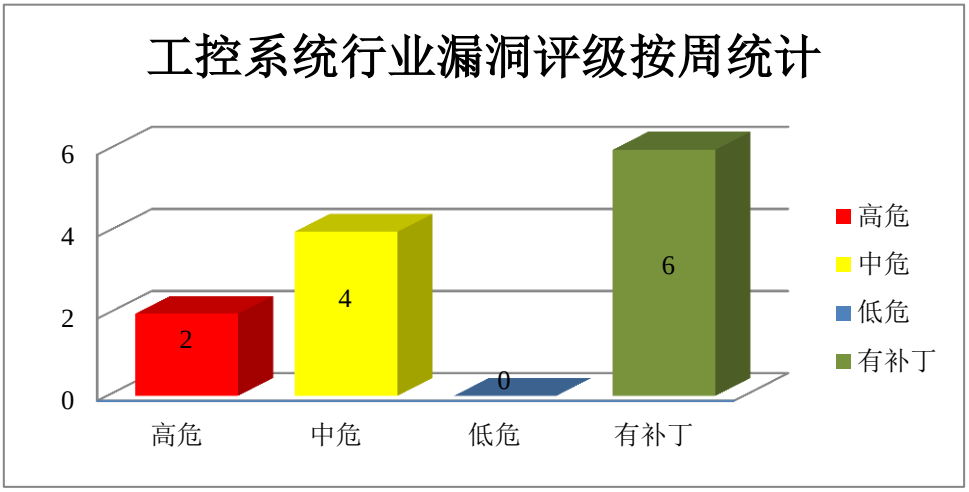

图 5 工控行业漏洞统计

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、Android 平台 WebView 控件存在高危漏洞

WebView 是 Android 用于显示网页的控件。本周，该产品被披露存在跨域访问高危漏洞，攻击者通过 URL Scheme 的方式，可远程打开并加载恶意 HTML 文件，远程获取 APP 中包括用户登录凭证在内的所有本地敏感数据。

CNVD 收录的相关漏洞包括：Android WebView 存在跨域访问漏洞。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-2017-36682

2、Microsoft 产品安全漏洞

Microsoft Windows 10 是一套供个人电脑使用的操作系统，Windows Server 2016 是一套服务器操作系统。Edge 是其中的一个系统附带的默认浏览器。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-2018-00504、CNVD-2018-00505、CNVD-2018-00506、CNVD-2018-00507、CNVD-2018-00508、CNVD-2018-00509、CNVD-2018-00510、CNVD-2018-00511）。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-2018-00504

http://www.cnvd.org.cn/flaw/show/CNVD-2018-00505

http://www.cnvd.org.cn/flaw/show/CNVD-2018-00506

http://www.cnvd.org.cn/flaw/show/CNVD-2018-00507

http://www.cnvd.org.cn/flaw/show/CNVD-2018-00508

http://www.cnvd.org.cn/flaw/show/CNVD-2018-00509

http://www.cnvd.org.cn/flaw/show/CNVD-2018-00510

http://www.cnvd.org.cn/flaw/show/CNVD-2018-00511

3、Google 产品安全漏洞

Android 是美国谷歌公司的一套以 Linux 为基础的开源操作系统。Media Framework 是其中的一个用于多媒体开发框架。Android Runtime（ART）是 Android 系统的运行环境。本周，上述产品被披露存在权限提升和远程代码执行漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Google Android Media Framework 权限提升漏洞（CNVD-2018-00624、CNVD-2018-00634、CNVD-2018-00635、CNVD-2018-00636）、Google Android Media Framework 远程代码执行漏洞（CNVD-2018-00631、CNVD-2018-00632、CNVD-2018-00633）、Google Android Runtime 权限提升漏洞。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-2018-00624

http://www.cnvd.org.cn/flaw/show/CNVD-2018-00634

http://www.cnvd.org.cn/flaw/show/CNVD-2018-00635

http://www.cnvd.org.cn/flaw/show/CNVD-2018-00636

http://www.cnvd.org.cn/flaw/show/CNVD-2018-00631

http://www.cnvd.org.cn/flaw/show/CNVD-2018-00632

http://www.cnvd.org.cn/flaw/show/CNVD-2018-00633

http://www.cnvd.org.cn/flaw/show/CNVD-2018-00649

4、PHP Scripts Mall 产品安全漏洞

PHP Scripts Mall Single Theater Booking 是一款开源剧院脚本；Car Rental Script 是一款用于出租车预订业主和代理的开源网站脚本；Resume Clone Script 是一款简历克隆脚本；Professional Service Script 是一款具有搜索、任务创建及任务管理功能的脚本。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数据库敏感信息或发起跨站脚本攻击等。

CNVD 收录的相关漏洞包括：PHP Scripts Mall Car Rental Script 跨站脚本漏洞、PHP Scripts Mall Car Rental Script 跨站请求伪造漏洞、PHP Scripts Mall Car Rental Script SQL 注入漏洞（CNVD-2018-00484）、PHP Scripts Mall Professional Service Script 跨站脚本漏洞、PHP Scripts Mall Professional Service Script 信息泄露漏洞、PHP Scripts Mall Professional Service Script SQL 注入漏洞（CNVD-2018-00489）、PHP Scripts Mall Resume Clone Script SQL 注入漏洞（CNVD-2018-00492）、PHP Scripts Mall

Single Theater Booking SQL 注入漏洞。除“PHP Scripts Mall Car Rental Script 跨站脚本漏洞、PHP Scripts Mall Car Rental Script 跨站请求伪造漏洞、PHP Scripts Mall Professional Service Script 跨站脚本漏洞、PHP Scripts Mall Professional Service Script 信息泄露漏洞”外，其余漏洞的综合评级为“高危”。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-2018-00485

http://www.cnvd.org.cn/flaw/show/CNVD-2018-00483

http://www.cnvd.org.cn/flaw/show/CNVD-2018-00484

http://www.cnvd.org.cn/flaw/show/CNVD-2018-00490

http://www.cnvd.org.cn/flaw/show/CNVD-2018-00488

http://www.cnvd.org.cn/flaw/show/CNVD-2018-00489

http://www.cnvd.org.cn/flaw/show/CNVD-2018-00492

http://www.cnvd.org.cn/flaw/show/CNVD-2018-00499

5、 Linksys WVBR0 无线网桥远程命令执行漏洞

Linksys WVBR0 是一款无线网络中继器设备。本周，Linksys 被披露存在远程命令执行漏洞，远程攻击者可利用该漏洞以 root 权限执行任意代码。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_-2018-00537

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-2018-00578	EMC Isilon OneFS 提权漏洞	高	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：http://www.emc.com
CNVD-2018-00595	Palo Alto Networks Global Protect Client 本地权限提升漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://securityadvisories.paloaltonetworks.com/Home/Detail/108
CNVD-2018-00646	GNU C Library 权限提升漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://sourceware.org/ml/libc-alpha/2017-12/msg00528.html
CNVD-2018-00672	Advantech WebAccess 输入验证漏洞	高	目前厂商已发布漏洞修复程序，请及时关注更新：http://www.advantech.com/industrial-automation/webaccess/download
CNVD-201	Advantech WebAccess SQL 注	高	目前厂商已发布升级补丁以修复漏

8-00669	入漏洞（CNVD-2018-00669）		洞，详情请关注厂商主页：http://www.advantech.com/
CNVD-2018-00710	picoTCP 栈缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/tass-belgium/picotcp/pull/473
CNVD-2018-00711	Sangoma NetBorder/Vega Session Controller 命令执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：ftp://ftp.sangoma.com/nsc/2.3/Changelog
CNVD-2018-00767	pidusage 命令注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.npmjs.com/package/pidusage
CNVD-2018-00852	International Components for Unicode (ICU) for C/C++堆栈缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/znc/znc/issues/1459
CNVD-2018-00859	Mozilla Thunderbird for Windows 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：https://www.mozilla.org/en-US/security/advisories/mfsa2017-30/

小结：本周，Android WebView 被披露存在跨域访问高危漏洞，攻击者通过 URL Scheme 的方式，可远程打开并加载恶意 HTML 文件，远程获取 APP 中包括用户登录凭证在内的所有本地敏感数据。此外，Microsoft、Google、PHP Scripts Mall 等多款产品被披露存在多个漏洞，攻击者可利用漏洞泄露数据库敏感信息、执行任意代码或发起跨站脚本攻击等。另外，Linksys 被披露存在远程命令执行漏洞，远程攻击者可利用该漏洞以 root 权限执行任意代码。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。

本周漏洞要闻速递

1. AMD 安全处理器被发现存在栈溢出漏洞

显然，近期大家的关注点都在 Meltdown 与 Spectre 漏洞上，谷歌也发出声明称漏洞影响了几乎所有的 CPU。而在同一天，谷歌云安全团队的安全研究员 Cfir Cohen 披露了 AMD 的安全处理器（PSP）的可信平台模块 TMP 中一个栈溢出漏洞。研究人员声称，攻击者可以使用特制的 EK 证书来获得 AMD 安全处理器上的代码执行权，从而危及其安全性。

参考链接：http://www.freebuf.com/news/159555.html

2. 西部数据 NAS 设备被曝存在硬编码后门和未授权文件上传高危漏洞

近日，GulfTech 公司安全研究员 James Bercegay 发现，西部数据（Western Digital）旗下多个 MyCloud 系列网络存储设备（WDMyCloud NAS）存在未限制文件上传、硬编码后门、CSRF、命令注入等多个高危漏洞，攻击者可以利用这些漏洞，对 MyCloud NAS 设备植入恶意代码，远程登录或获得设备控制权限（漏洞利用 exploit）。而且，WDMyCloud 竟然还与 D-Link 存在代码共用情况！

参考链接：http://www.freebuf.com/news/160039.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