

信息安全漏洞周报

2018 年 3 月 12 日-2018 年 3 月 18 日

2018 年第 11 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 460 个，其中高危漏洞 130 个、中危漏洞 292 个、低危漏洞 38 个。漏洞平均分为 5.64。本周收录的漏洞中，涉及 0day 漏洞 68 个（占 15%），其中互联网上出现“WordPress 拒绝服务漏洞（CNVD-2018-05439）、MalwareFox AntiMalware 本地权限提升漏洞”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 622 个，与上周（641 个）环比下降 3%。

CNVD收录漏洞近10周平均分分布图

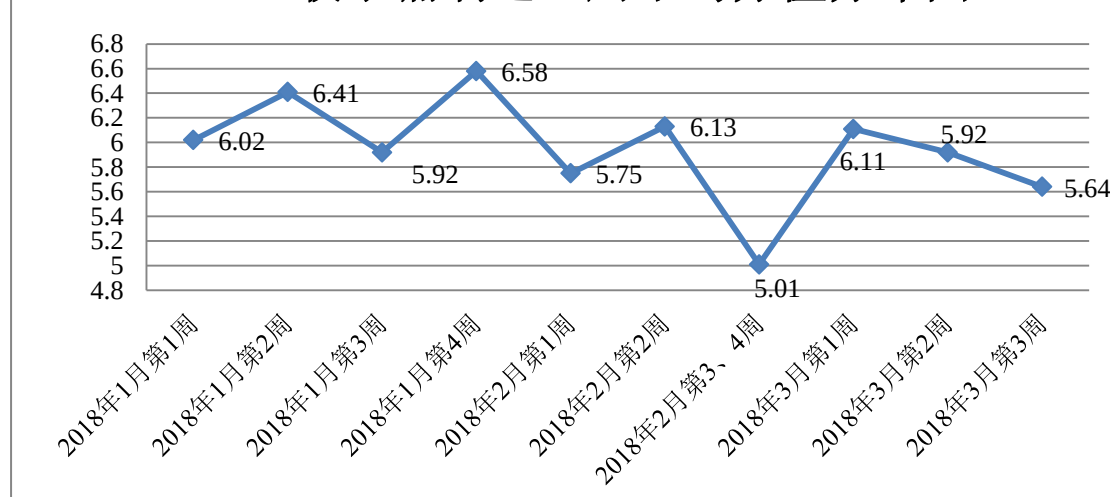


图 1 CNVD 收录漏洞近 10 周平均分分布图

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、哈尔滨安天科技股份有限公司、华为技术有限公司、恒安嘉新(北京)科技股份公司、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。四川虹微技术有限公司（子午攻防实验室）、

上海观安信息技术股份有限公司、中新网络信息安全股份有限公司、福建省海峡信息技术有限公司、安徽三实信息技术服务有限公司、南京联成科技发展股份有限公司、漏斗社区、江西神舟信息安全评估中心、常州瑞新网络科技股份有限公司、南瑞集团公司（国网电力科学研究院）、北京同余科技有限公司、福建榕基软件股份有限公司、邹平九零冰讯网络科技有限公司及其他个人白帽子向 CNVD 提交了 622 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 324 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
北京天融信网络安全技术有限公司	228	1
哈尔滨安天科技股份有限公司	200	0
360 网神（补天平台）	168	168
华为技术有限公司	168	0
漏洞盒子	156	156
恒安嘉新(北京)科技股份有限公司	89	0
新华三技术有限公司	89	0
中国电信集团系统集成有限责任公司	47	0
北京数字观星科技有限公司	38	0
北京神州绿盟科技有限公司	35	0
卫士通信息产业股份有限公司	17	0
北京无声信息技术有限公司	15	0
蓝盾信息安全技术有限公司	2	2
深圳市深信服电子科技有限公司	1	1
四川虹微技术有限公司（子午攻防实验室）	56	56
上海观安信息技术股份有限公司	25	25

中新网络信息安全股份有限公司	9	9
福建省海峡信息技术有限公司	8	8
安徽三实信息技术服务有限公司	5	5
南京联成科技发展股份有限公司	5	5
漏斗社区	4	4
江西神舟信息安全评估中心	3	3
常州瑞新网络科技股份有限公司	2	2
南瑞集团公司（国网电力科学研究院）	2	2
北京同余科技有限公司	1	1
福建榕基软件股份有限公司	1	1
邹平九零冰讯网络科技有限公司	1	1
CNCERT 湖南分中心	8	8
CNCERT 吉林分中心	3	3
CNCERT 宁夏分中心	2	2
CNCERT 河北分中心	2	2
CNCERT 甘肃分中心	1	1
CNCERT 陕西分中心	1	1
CNCERT 海南分中心	1	1
个人	154	154
报送总计	1547	622

本周漏洞按类型和厂商统计

本周，CNVD 收录了 460 个漏洞。其中应用程序漏洞 323 个，WEB 应用漏洞 52 个，网络设备漏洞 48 个，操作系统漏洞 32 个，安全产品漏洞 4 个，数据库漏洞 1 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	323
WEB 应用漏洞	52
网络设备漏洞	48
操作系统漏洞	32
安全产品漏洞	4
数据库漏洞	1

本周CNVD漏洞数量按影响类型分布

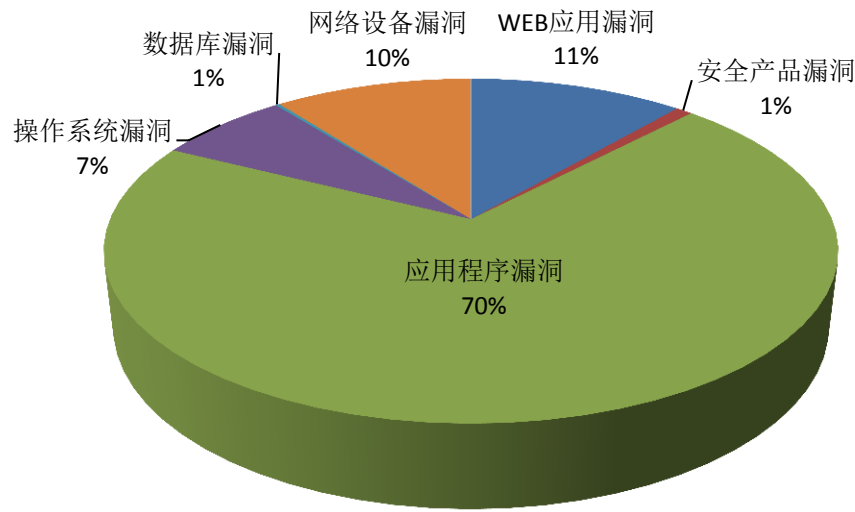


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、Cisco、Wireshark 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	Adobe	45	10%
2	Cisco	35	7%
3	Wireshark	24	5%
4	Huawei	21	5%
5	Microsoft	15	3%
6	HP	13	3%
7	libming	12	3%
8	Schneider Electric	12	3%
9	GNU	11	2%

10	其他	272	59%
----	----	-----	-----

本周行业漏洞收录情况

本周，CNVD 收录了 12 个电信行业漏洞，14 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，“Google Android Kernel 组件权限提升漏洞（CNVD-2018-05460）、OSIs oft PI Web API 权限提升漏洞、Siemens 多个产品文件上传漏洞、OSIs oft PI Data Archive 权限提升漏洞、Google Android Qualcomm 组件权限提升漏洞（CNVD-2018-05458）”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/>

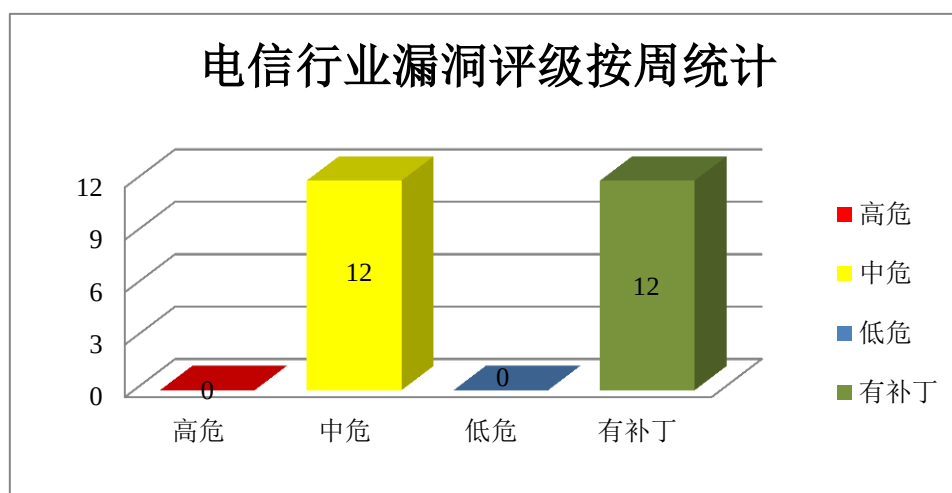


图 3 电信行业漏洞统计

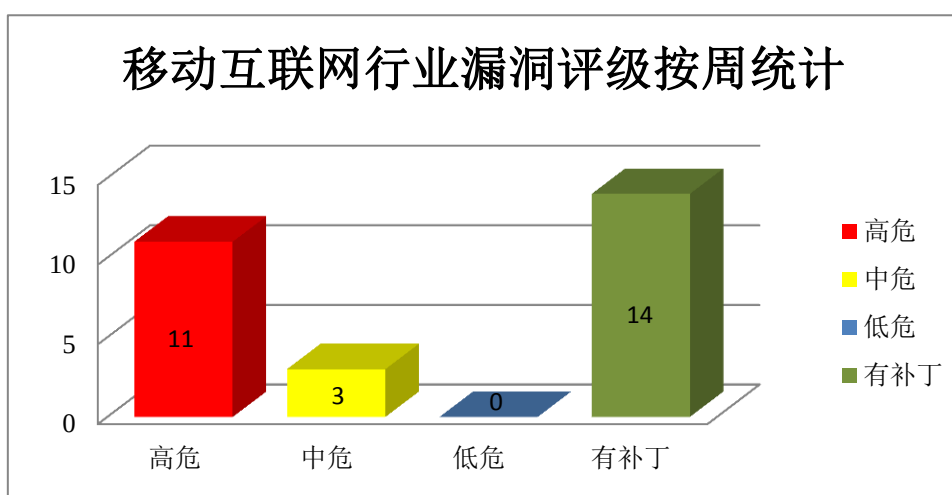


图 4 移动互联网行业漏洞统计

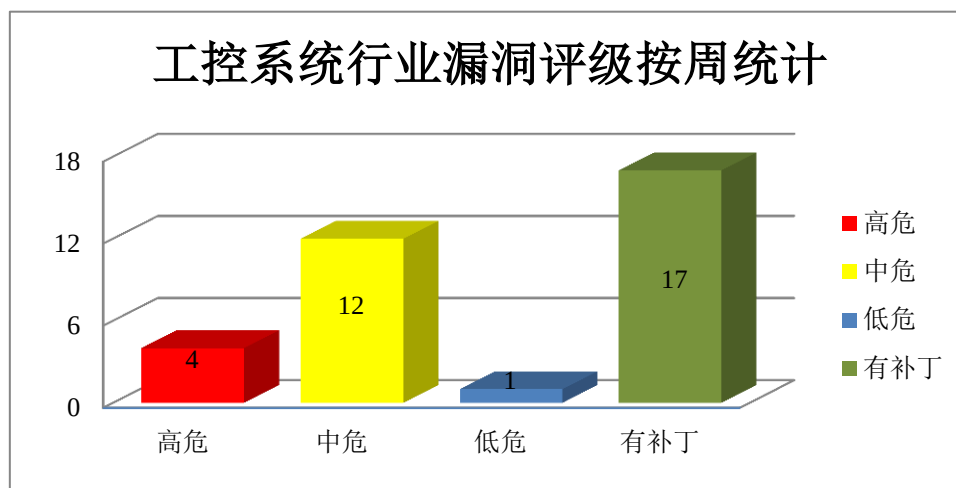


图 5 工控行业漏洞统计

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、Adobe 产品安全漏洞

Acrobat DC Continuous Track 等都是美国奥多比（Adobe）公司的产品。Acrobat DC Continuous Track 是一款桌面版 PDF 解决方案的连续更新版本。Reader DC Continuous Track 是一款 PDF 阅读工具的连续更新版本。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：多款 Adobe 产品越界内存读取漏洞（CNVD-2018-05018、CNVD-2018-05019、CNVD-2018-05020、CNVD-2018-05021、CNVD-2018-05022、CNVD-2018-05023、CNVD-2018-05024、CNVD-2018-05025）。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-2018-0518>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-0519>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-0520>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-0521>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-0522>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-0523>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-0524>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-0525>

2、Microsoft 产品安全漏洞

Microsoft Windows 是美国微软公司发布的一系列操作系统。Windows kernel 是其中的一个操作系统内核。Microsoft Outlook 是一套 Office 套件中的电子邮件客户端软件。

Office Click-to-Run (C2R) 是一套办公软件套件产品。本周，上述产品被披露存在权限提升、代码执行和内存破坏漏洞，攻击者可利用漏洞提升权限或执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Office 2016 Click-to-Run 远程代码执行漏洞、Microsoft Outlook 内存破坏漏洞、Microsoft Windows kernel 权限提升漏洞（CNVD-2018-05033、CNVD-2018-05037、CNVD-2018-05038、CNVD-2018-05039、CNVD-2018-05040、CNVD-2018-05041）。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-2018-05035>
<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05036>
<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05033>
<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05037>
<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05038>
<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05039>
<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05040>
<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05041>

3、Google 产品安全漏洞

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。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 Kernel 组件权限提升漏洞（CNVD-2018-05460）、Google Android Qualcomm 组件权限提升漏洞（CNVD-2018-05452、CNVD-2018-05453、CNVD-2018-05454、CNVD-2018-05455、CNVD-2018-05456、CNVD-2018-05457、CNVD-2018-05458）。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-2018-05460>
<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05452>
<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05453>
<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05454>
<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05455>
<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05456>
<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05457>
<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05458>

4、Schneider Electric 产品安全漏洞

Schneider Electric Pelco Sarix Professional 是法国施耐德电气公司的一款视频监控

设备。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞执行任意命令、提升权限或下载任意文件等。

CNVD 收录的相关漏洞包括：Schneider Electric Pelco Sarix Professional 缓冲区溢出漏洞、Schneider Electric Pelco Sarix Professional 命令执行漏洞、Schneider Electric Pelco Sarix Professional 命令执行漏洞（CNVD-2018-05325、CNVD-2018-05326）、Schneider Electric Pelco Sarix Professional 权限提升漏洞、Schneider Electric Pelco Sarix Professional 权限提升漏洞（CNVD-2018-05321）、Schneider Electric Pelco Sarix Professional 任意文件删除漏洞、Schneider Electric Pelco Sarix Professional 任意文件下载漏洞。除“Schneider Electric Pelco Sarix Professional 任意文件删除漏洞、Schneider Electric Pelco Sarix Professional 任意文件下载漏洞”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-2018-05331>
<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05327>
<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05325>
<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05326>
<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05322>
<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05321>
<http://www.cnvd.org.cn/flaw/show/CNVD-2018-04332>
<http://www.cnvd.org.cn/flaw/show/CNVD-2018-05329>

5、OMRON NS 设备认证绕过漏洞

OMRON NS devices 是欧姆龙（Omron）公司的一款触摸屏人机界面编程设备。本周，OMRON 被披露存在认证绕过漏洞，远程攻击者可通过向.html 文件发送直接请求利用该漏洞绕过身份验证。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-2018-05425>

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-2018-05205	powerpc 和 Intel i386 GNU C Library 整数溢出漏洞	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： https://www.gnu.org/
CNVD-2018-05226	DS Data Systems KonaKart e Commerce Platform 目录遍历漏洞	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： https://www.konakart.com/

CNVD-2018-05440	mini_httpd 和 tthttpd 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://acme.com/updates/archive/199.html
CNVD-2018-05468	Apport 拒绝服务漏洞（CNVD-2018-05468）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://usn.ubuntu.com/usn/usn-3480-1/
CNVD-2018-05469	Apport 拒绝服务漏洞（CNVD-2018-05469）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://usn.ubuntu.com/usn/usn-3480-1/
CNVD-2018-05486	Trend Micro Control Manager 身份验证绕过漏洞	高	厂商已发布漏洞修复程序，请及时关注更新： https://success.trendmicro.com/solution/1119158
CNVD-2018-05487	OpenEMR fax_dispatch.php 文件 OS 命令注入漏洞	高	厂商已发布漏洞修复程序，请及时关注更新： http://www.open-emr.org/wiki/index.php/OpenEMR_Patches
CNVD-2018-05511	web2py sample Web 应用程序命令执行漏洞	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.web2py.com/
CNVD-2018-05517	Apport 拒绝服务漏洞（CNVD-2018-05517）	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： https://wiki.ubuntu.com/Apport
CNVD-2018-05521	web2py 任意代码执行漏洞	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.web2py.com/

小结：本周，Adobe 被披露存在多个漏洞，攻击者可利用漏洞执行任意代码。此外，Google、Microsoft、Schneider Electric 等多款产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码、提升权限或删除任意文件等。另外，OMRON 被披露存在认证绕过漏洞，远程攻击者可通过向.html 文件发送直接请求利用该漏洞绕过身份验证。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. Sublime、Vim 等多款流行文本编辑器存在特权升级漏洞

在最近一系列利用漏洞插件的攻击之后，SafeBreach 的研究人员探讨了具有第三方可扩展性机制的高级文本编辑器如何被滥用来提升设备权限，并针对 Unix 和 Linux 系统检查了几种流行的可扩展文本编辑器（Sublime、Vim、Emacs、Gedit、pico / nano）。经过研究发现，除 pico / nano 之外，所有受检查的编辑器都受到了一个关键的特权升级漏洞影响，攻击者可以利用这个漏洞在运行易受攻击的文本编辑器的目标设备上运行

恶意代码。

参考链接: <https://www.easyaq.com/news/161647415.shtml>

2. 英特尔八代至强和酷睿处理器将彻底解决熔断和幽灵漏洞

英特尔 CEO Brian Krzanich 今天宣布,下一代至强 Scalable (Cascade Lake) 处理器和第八代英特尔酷睿处理器将采用全新设计的组件,并解决了“Meltdown”(熔断)和“Spectre”(幽灵)漏洞。“Spectre”(幽灵)变种 1 仍然需要通过软件解决。英特尔的下一代处理器将通过硬件设计的变化解决“Spectre”(幽灵)变种 2 和“Meltdown”(熔断)变种 3。

参考链接: <https://www.easyaq.com/news/275092902.shtml>

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