

信息安全漏洞周报

2017 年 08 月 07 日-2017 年 08 月 13 日

2017年第33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 302 个，其中高危漏洞 107 个、中危漏洞 188 个、低危漏洞 7 个。漏洞平均分为 6.23。本周收录的漏洞中，涉及 0day 漏洞 169 个（占 56%），其中互联网上出现“Motorola MX011ANM Comcast 固件设计缺陷漏洞、WordPress Etoile Ultimate Product Catalog 插件 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 1665 个，与上周（2257 个）环比下降 26%

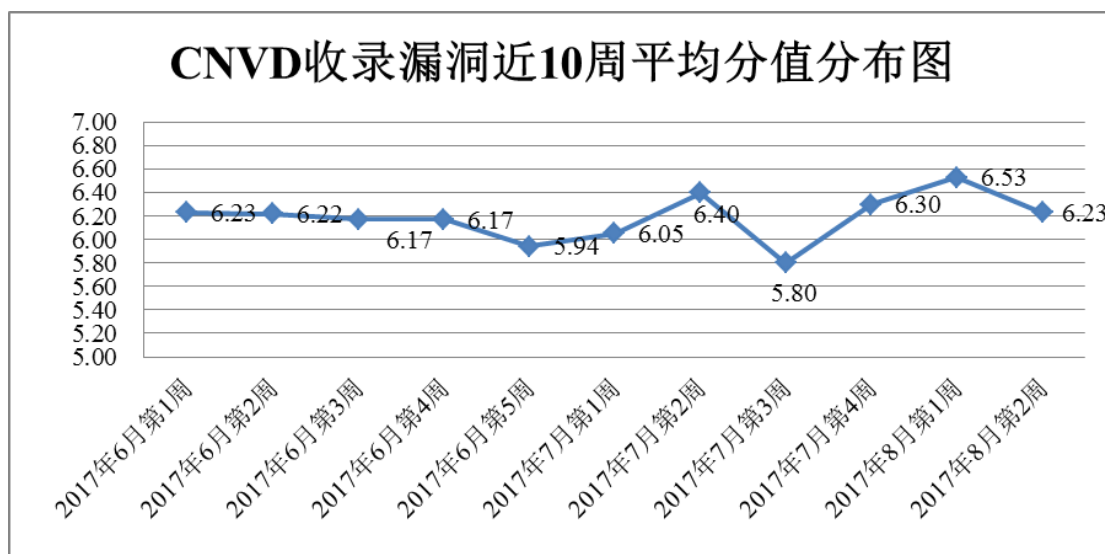


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周，共 16 家成员单位、企业用户及个人用户报送了本周收录的全部 302 个漏洞。报送情况如表 1 所示。其中，天融信、东软、华为技术有限公司、安天实验室、恒安嘉新等单位报送数量较多。360 网神、漏洞盒子、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、山石网科通信技术有限公司、广州软云计算机科技有限公司、深圳市鼎安天下信息科技有限公司、安徽新华博信息技术股份有限公司、北京安码科技有限公司、君立华域、六壬网安、广州神月信息安全技术有限公司、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 1665 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
天融信	425	0
360 网神	348	348
东软	334	2
华为技术有限公司	294	0
安天实验室	193	0
恒安嘉新	185	0
H3C	179	0
中国电信集团系统集成有 限责任公司	136	31
北京数字观星科技有限公 司	87	0
绿盟科技	85	0
厦门服云信息科技有限公 司	79	1
启明星辰	70	6
杭州安恒信息技术有限公 司	55	0
漏洞盒子	34	34
知道创宇	4	2
广西鑫瀚科技有限公司	2	2
南京联成科技发展股份有 限公司	29	29
中新网络信息安全股份有 限公司	15	15
山石网科通信技术有限公 司	11	11

广州软云计算机科技有限公司	10	10
深圳市鼎安天下信息科技有限公司	9	9
安徽新华博信息技术股份有限公司	8	8
北京安码科技有限公司	8	8
君立华域	8	8
六壬网安	2	2
广州神月信息安全技术有限公司	1	1
上海零盾网络科技有限公司	1	1
CNCERT 宁夏分中心	12	12
CNCERT 浙江分中心	2	2
CNCERT 广东分中心	2	2
CNCERT 上海分中心	1	1
个人	1120	1120
报送总计	3749	1665
录入总计	302（去重）	1665

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 302 个漏洞。其中应用程序漏洞 158 个，web 应用漏洞 84 个，网络设备漏洞 33 个，操作系统漏洞 20 个，安全产品漏洞 4 个，数据库漏洞 3 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	158
web 应用漏洞	84
网络设备漏洞	33
操作系统漏洞	20
安全产品漏洞	4
数据库漏洞	3

表 2 漏洞按影响类型统计表

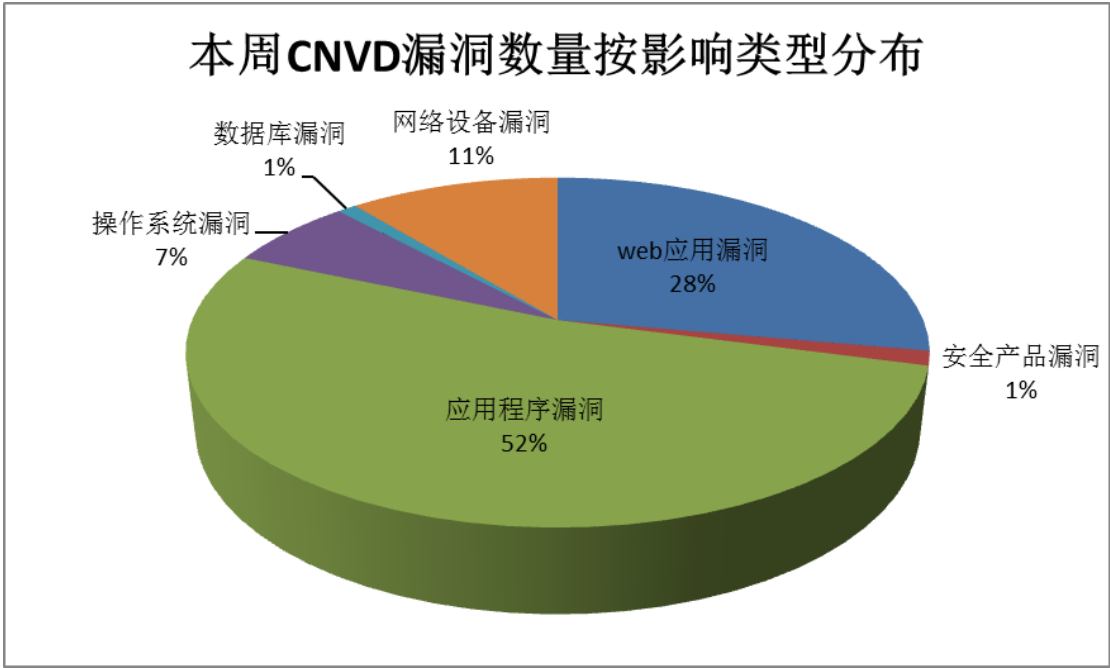


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、Microsoft、Trend Micro 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	Oracle	20	7%
2	Microsoft	20	7%
3	Trend Micro	12	4%
4	Advantech	10	3%
5	GraphicsMagick	10	3%
6	Cisco	9	3%
7	Huawei	9	3%
8	Motorola	9	3%
9	ImageMagick	7	2%
10	其他	196	65%

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 23 个电信行业漏洞，15 个移动互联网行业漏洞，10 个工控系统行业漏洞（如下图所示）。其中，“Microsoft SQL Server 信息泄露漏洞（CNVD-2017-20513）、I-O DATA WN-AX1167GR 操作系统命令注入漏洞、D-Link DIR 系列路由器

远程命令执行漏洞、Huawei honor 6x 驱动程序缓冲区溢出漏洞、多款 Huawei 手机缓冲区溢出漏洞”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/>

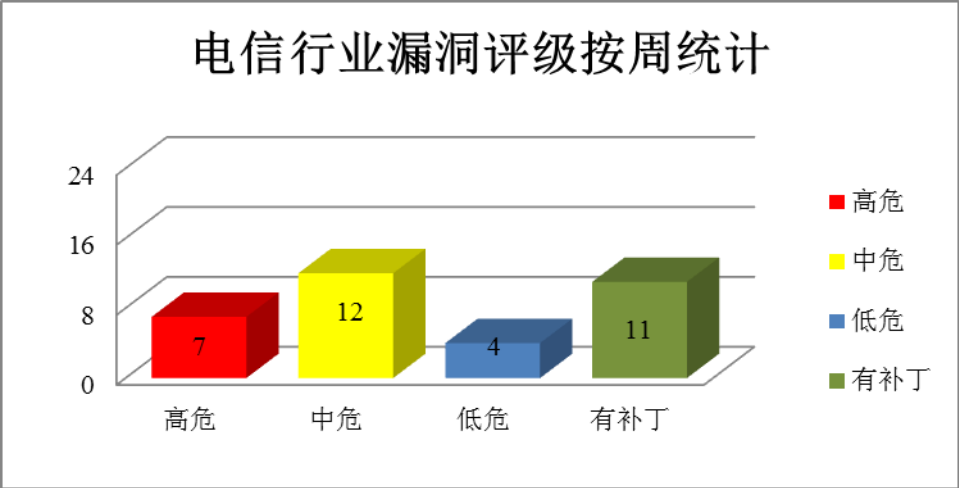


图 3 电信行业漏洞统计

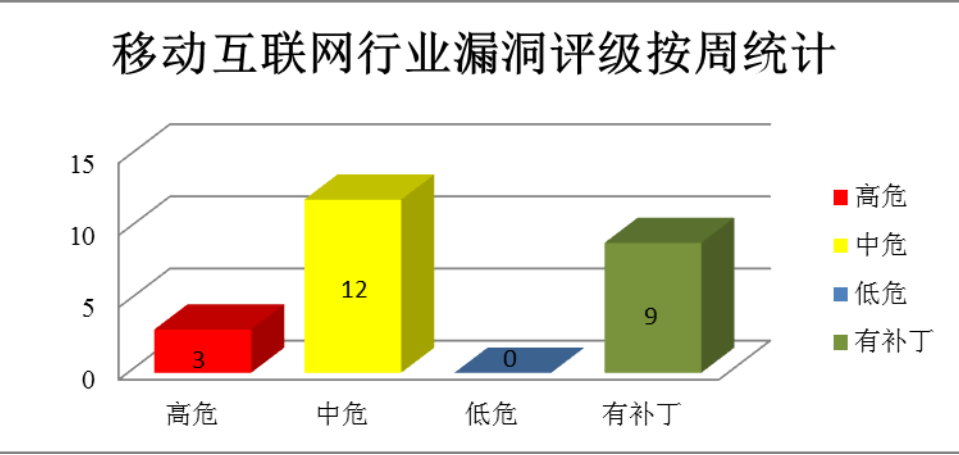


图 4 移动互联网行业漏洞统计

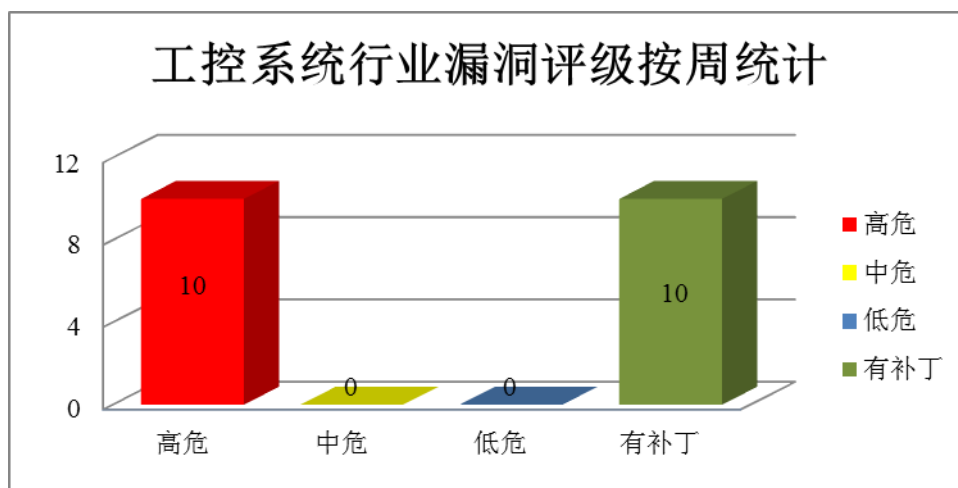


图 5 工控系统行业漏洞统计

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、D-Link DIR 系列路由器存在多个漏洞

DIR 系列是友讯（D-Link）公司的一系列云路由器产品本周，该产品被披露存在远程命令执行和信息泄露漏洞，攻击者可利用漏洞执行任意代码或泄露敏感信息。

CNVD 收录的相关漏洞包括：D-Link DIR 系列路由器远程命令执行漏洞、D-Link DIR 系列路由器身份验证信息泄露漏洞。其中“D-Link DIR 系列路由器远程命令执行漏洞”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-2017-20001>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-20002>

2、Microsoft 产品安全漏洞

Microsoft Windows 10 是美国微软（Microsoft）公司发布的一套新一代跨平台操作系统。Microsoft Edge 是其中的一个系统附带的默认浏览器。JavaScript engines 是其中的一个 JavaScript 引擎组件。本周，上述产品被披露存在安全绕过、权限提升和远程代码执行漏洞，攻击者可利用漏洞绕过安全限制、提升权限或执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Edge 安全绕过漏洞（CNVD-2017-20503）、Microsoft Edge 权限提升漏洞（CNVD-2017-20514）、Microsoft Windows 10 Edge JavaScript 远程代码执行漏洞、Microsoft Windows 10 Edge JavaScript 远程代码执行漏洞（CNVD-2017-20506）、Microsoft Windows Edge JavaScript 引擎远程代码执行漏洞、Microsoft Windows Edge JavaScript 引擎远程代码执行漏洞（CNVD-2017-20499、CNVD-2017-20500、CNVD-2017-20501）。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-2017-20503>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-20514>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-20502>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-20506>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-20498>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-20499>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-20500>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-20501>

3、Oracle 产品安全漏洞

Oracle Fusion Middleware 是美国甲骨文公司的一套面向企业和云环境的业务创新平台。Oracle Java SE 是一套标准版 Java 平台。Oracle Sun Systems Products Suite 是一款 Sun 系统产品套件。Oracle PeopleSoft Products 是一套企业人力资本管理解决方案。本周, 上述产品被披露存在多个漏洞, 攻击者可利用漏洞影响数据的可用性、保密性和完整性。

CNVD 收录的相关漏洞包括: Oracle Business Intelligence Enterprise Edition 存在未明漏洞、Oracle Java Advanced Management Console 存在未明漏洞、Oracle Service Bus 存在未明漏洞、Oracle Sun Systems Products Suite Solaris 存在未明漏洞、Oracle PeopleSoft Enterprise PeopleTools 存在未明漏洞 (CNVD-2017-20279、CNVD-2017-20289、CNVD-2017-20291)、Oracle PeopleSoft Enterprise FSCM 存在未明漏洞。其中 “Oracle Business Intelligence Enterprise Edition 存在未明漏洞、Oracle Java Advanced Management Console 存在未明漏洞、Oracle Service Bus 存在未明漏洞、Oracle Sun Systems Products Suite Solaris 存在未明漏洞” 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-2017-20280>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-20288>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-20296>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-20290>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-20279>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-20289>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-20291>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-20281>

4、Huawei 产品安全漏洞

Huawei honor 6x 和 honor 5C、Huawei P10 和 P10 Plus 等都是中国华为公司的一

款智能手机。本周，上述产品被披露存在拒绝服务和缓冲区溢出漏洞，攻击者可利用漏洞发起拒绝服务攻击或执行任意代码。

CNVD 收录的相关漏洞包括：Huawei honor 6x 驱动程序缓冲区溢出漏洞、Huawei 手机通话模块拒绝服务漏洞、Huawei 手机通话模块拒绝服务漏洞（CNVD-2017-19188）、多款 Huawei 手机缓冲区溢出漏洞、多款 Huawei 手机缓冲区溢出漏洞（CNVD-2017-19191、CNVD-2017-19192、CNVD-2017-19193、CNVD-2017-19194）。除“Huawei 手机通话模块拒绝服务漏洞、Huawei 手机通话模块拒绝服务漏洞（CNVD-2017-19188）”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-2017-19189>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-19187>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-19188>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-19190>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-19191>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-19192>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-19193>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-19194>

5、NetComm Wireless 4GT101W 路由器信息泄露漏洞

NetComm Wireless 4GT101W routers 是澳大利亚 NetComm Wireless 公司的一款无线路由器产品。本周，NetComm 被披露存在信息泄露漏洞，攻击者可利用漏洞获取敏感信息。目前，互联网上已经出现了针对该漏洞的攻击代码，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-2017-19556>

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-2017-19550	GLPI front/devicesoundcard.php 文件 SQL 注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://github.com/glpi-project/glpi/issues/2449
CNVD-2017-19974	GraphicsMagick 缓冲区溢出漏洞（CNVD-2017-19974）	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.graphicsmagick.org/
CNVD-2017-19976	GraphicsMagick 内存泄露漏洞（CNVD-2017-19976）	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.graphicsmagick.org/
CNVD-201	GraphicsMagick 拒绝服务漏洞	高	目前厂商已发布升级补丁以修复漏

7-19978	(CNVD-2017-19978)		洞，详情请关注厂商主页： http://www.graphicsmagick.org/
CNVD-2017-19979	GraphicsMagick 缓冲区溢出漏洞 (CNVD-2017-19979)	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.graphicsmagick.org/
CNVD-2017-20299	Trend Micro Control Manager SQL 注入漏洞 (CNVD-2017-20299)	高	厂商已发布漏洞修复程序，请及时关注更新： https://success.trendmicro.com/solution/1117722
CNVD-2017-20300	Trend Micro Control Manager SQL 注入漏洞 (CNVD-2017-20300)	高	厂商已发布漏洞修复程序，请及时关注更新： https://success.trendmicro.com/solution/1117722
CNVD-2017-20417	Trend Micro Deep Discovery Director 命令注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://success.trendmicro.com/solution/111766
CNVD-2017-20421	Trend Micro Control Manager 目录遍历漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： https://success.trendmicro.com/solution/1117722
CNVD-2017-20455	ImageMagick 'ReadDCMImage' 函数拒绝服务漏洞	高	厂商已发布漏洞修复程序，请及时关注更新： http://www.imagemagick.org/download/beta/

表 4 部分重要高危漏洞列表

小结：本周，D-Link 被披露存在远程命令执行和信息泄露漏洞，攻击者可利用漏洞执行任意代码或泄露敏感信息。此外，Microsoft、Oracle、Huawei 等多款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、执行任意代码或发起拒绝服务攻击等。另外，NetComm 被披露存在信息泄露漏洞，攻击者可利用漏洞获取敏感信息。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. 许多常见 .NET 项目中存在的反序列化漏洞

2016 年 Java 应用程序及开发者受到反序列化漏洞的破坏性影响，而如今 .NET 生态系统也正在遭受同样的危机。新的问题存在于 .NET 代码库中处理反序列化的操作中，攻击者同样可以通过这个漏洞在服务器或相关计算机设备上进行了代码注入。研究人员发现在 .NET 数据管理后端框架 Breeze 中存在 JSON 反序列化漏洞。而除了 JSON 反序列化之外，还有一些 .NET 库中还存在着 XML 数据对象的反序列化问题。

参考链接: <http://www.freebuf.com/news/143609.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