国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2018 年 3 月 26 日-2018 年 4 月 01 日 **2018 年第 13 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 452 个，其中高危漏洞 134 个、中危漏洞 276 个、低危漏洞 42 个。漏洞平均分值为 5.75。本周收录的漏洞中，涉及 0day 漏洞 92 个（占 20%），其中互联网上出现“Zoho ManageEngine Applications Manager 远程代码执行漏洞（CNVD-2018-06478）、PHP Scripts Mall Schools Alert Management Script SQL 注入漏洞（CNVD-2018-06439）”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 391 个，与上周（438 个）环比下降 11%。

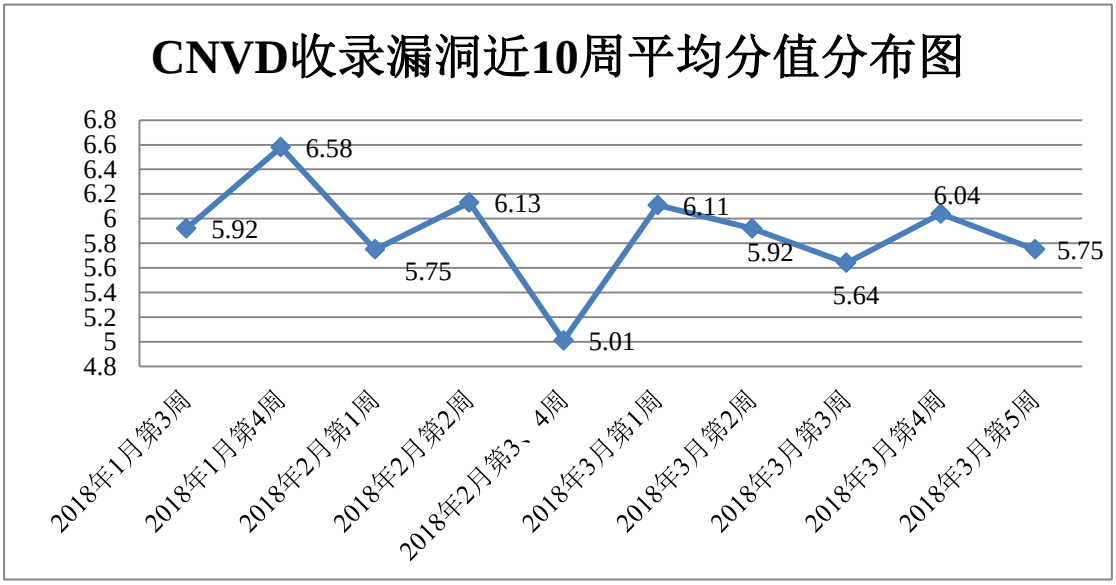

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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、哈尔滨安天科技股份有限公司、沈阳东软系统集成工程有限公司、华为技术有限公司、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。四川虹微技术有限公司（子午攻防实验室）、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、福建榕基软件股份有限公司、安徽三实信息技术服务有限公司、北京亚鸿世纪科技发展有限公司、南京联成科技发展股份有限公司、北京智游网安科技有限公司、广州万方计算机科技有限公司、上海观安信息技术股份有限公司、中国电信股份有限公司网络安全产品运营中心、漏斗社区、河北网信智安信息技术有限公司及其他个人白帽子向 CNVD 提交了 391 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 184 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	303	6
哈尔滨安天科技股份有限公司	217	0
沈阳东软系统集成工程有限公司	198	0
华为技术有限公司	167	0
漏洞盒子	137	137
新华三技术有限公司	105	0
北京数字观星科技有限公司	65	0
恒安嘉新(北京)科技股份公司	64	0
北京神州绿盟科技有限公司	48	0
360 网神（补天平台）	47	47
中国电信集团系统集成有限责任公司	32	0
北京无声信息技术有限公司	31	0
卫士通信息产业股份有限公司	14	0
蓝盾信息安全技术有限公司	1	1
北京知道创宇信息技术有限公司	1	0

四川虹微技术有限公司（子午攻防实验室）	28	28
中新网络信息安全股份有限公司	8	8
福建省海峡信息技术有限公司	7	7
福建榕基软件股份有限公司	3	3
安徽三实信息技术服务有限公司	3	3
北京亚鸿世纪科技发展有限公司	2	2
南京联成科技发展股份有限公司	2	2
北京智游网安科技有限公司	1	1
广州万方计算机科技有限公司	1	1
上海观安信息技术股份有限公司	1	1
中国电信股份有限公司网络安全产品运营中心	1	1
漏斗社区	1	1
河北网信智安信息技术有限公司	1	1
CNCERT 山西分中心	11	11
CNCERT 重庆分中心	6	6
CNCERT 上海分中心	3	3
CNCERT 浙江分中心	3	3
CNCERT 陕西分中心	3	3
CNCERT 河北分中心	3	3
CNCERT 天津分中心	2	2
CNCERT 吉林分中心	1	1
CNCERT 海南分中心	1	1

个人	108	108
报送总计	1630	391

本周漏洞按类型和厂商统计

本周，CNVD 收录了 487 个漏洞。其中应用程序漏洞 267 个，操作系统漏洞 75 个，WEB 应用漏洞 73 个，网络设备漏洞 30 个，安全产品漏洞 6 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	267
操作系统漏洞	75
WEB 应用漏洞	73
网络设备漏洞	30
安全产品漏洞	6
数据库漏洞	1

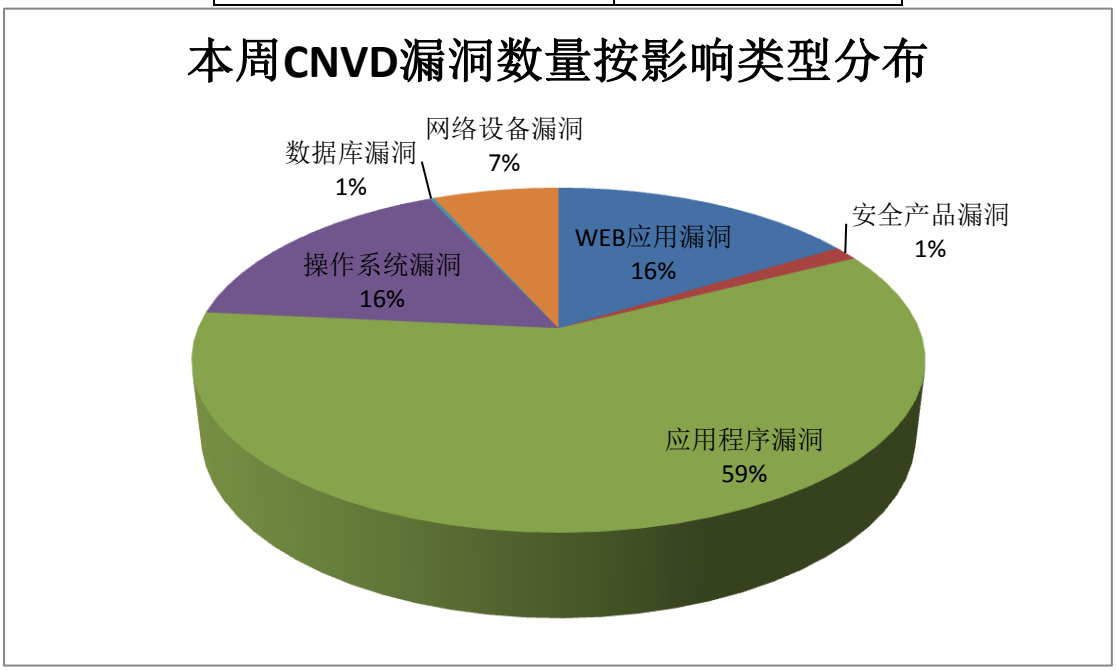

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Microsoft、Google、Google 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	40	9%
2	IBM	26	6%

3	Google	23	5%
4	Linux	19	4%
5	Cisco	15	3%
6	Apache	11	2%
7	Exempi	10	2%
8	Xpdf	8	2%
9	ZZCMS	7	2%
10	其他	293	65%

本周行业漏洞收录情况

本周，CNVD 收录了 24 个电信行业漏洞，34 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，“Beckhoff TwinCAT 不可信指针引用漏洞、ABB MicroSCADA 安装权限提升漏洞、多款 D-Link 产品操作系统命令注入漏洞、Cisco IOS 和 IOS XE 缓冲区溢出漏洞、Apple iOS、tvOS 和 watchOS Core Bluetooth 内存破坏漏洞”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/

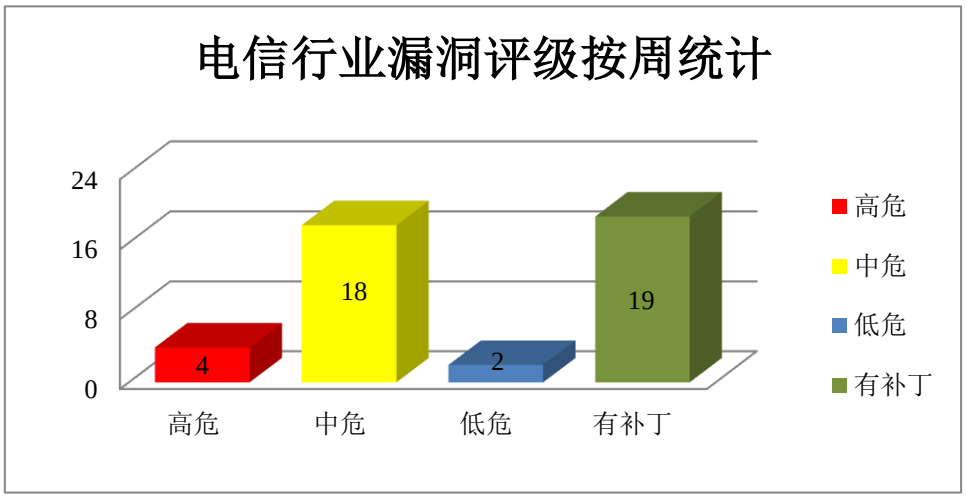

图 3 电信行业漏洞统计

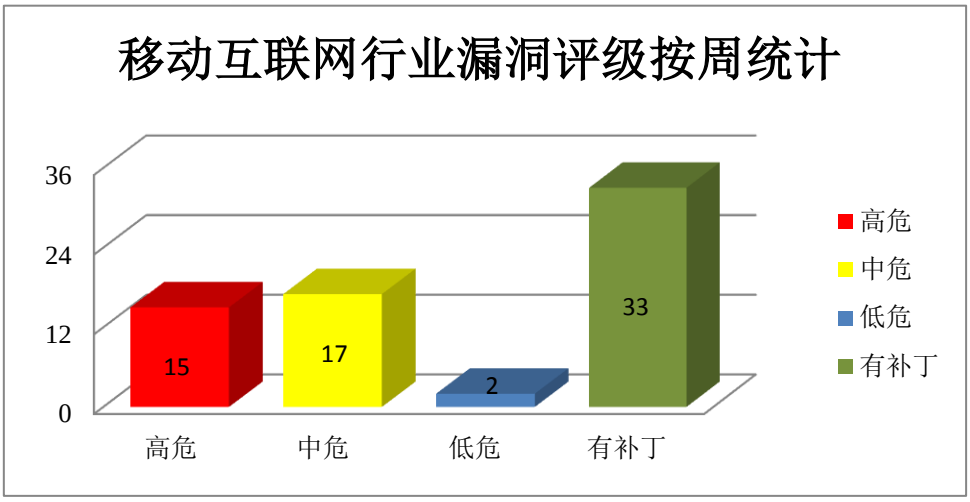

图 4 移动互联网行业漏洞统计

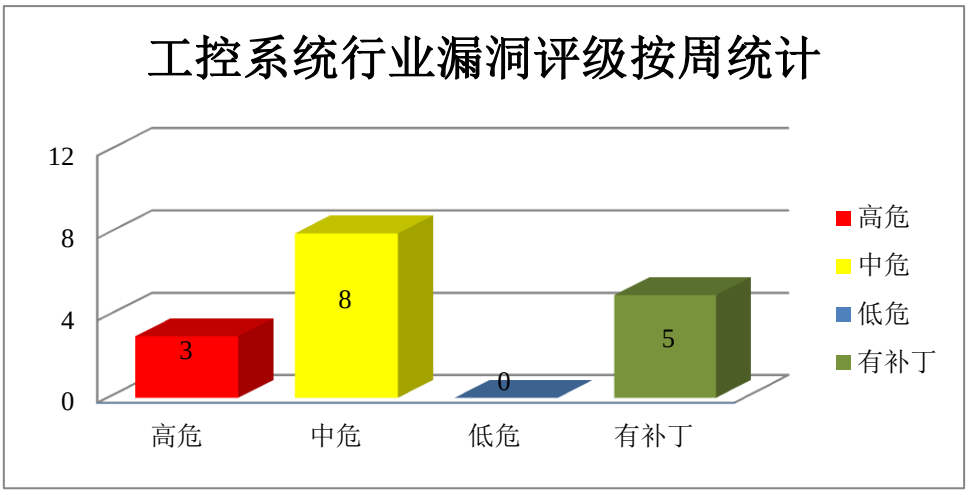

图 5 工控行业漏洞统计

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、Drupal 产品安全漏洞

Drupal 是 Drupal 社区所维护的一套用 PHP 语言开发的免费、开源的内容管理系统。本周，该产品被披露存在远程代码执行漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Drupal core 远程代码执行漏洞（CNVD-2018-06660）。该漏洞的综合评级为“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-2018-06660

2、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。本周，该产品被披露存在远程代码执行漏洞，攻击者可利用漏执行任意代码。

CNVD 收录的相关漏洞包括：Google Android Media framework 远程代码执行漏洞（CNVD-2018-06661、CNVD-2018-06662、CNVD-2018-06663、CNVD-2018-06664、CNVD-2018-06665、CNVD-2018-06666）、Google Android System 组件远程代码执行漏洞（CNVD-2018-06643、CNVD-2018-06644）。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-2018-06661
http://www.cnvd.org.cn/flaw/show/CNVD-2018-06662
http://www.cnvd.org.cn/flaw/show/CNVD-2018-06663
http://www.cnvd.org.cn/flaw/show/CNVD-2018-06664
http://www.cnvd.org.cn/flaw/show/CNVD-2018-06665
http://www.cnvd.org.cn/flaw/show/CNVD-2018-06666
http://www.cnvd.org.cn/flaw/show/CNVD-2018-06643
http://www.cnvd.org.cn/flaw/show/CNVD-2018-06644

3、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。Edge 是其中的一个系统附带的默认浏览器。Microsoft Internet Explorer（IE）是一款 Web 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或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Microsoft Edge 和 ChakraCore 远程内存破坏漏洞（CNVD-2018-06694、CNVD-2018-06695、CNVD-2018-06696、CNVD-2018-06697、CNVD-2018-06698、CNVD-2018-06699、CNVD-2018-06700）、Microsoft Internet Explorer 内存破坏漏洞（CNVD-2018-06313）。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-2018-06694
http://www.cnvd.org.cn/flaw/show/CNVD-2018-06695
http://www.cnvd.org.cn/flaw/show/CNVD-2018-06696
http://www.cnvd.org.cn/flaw/show/CNVD-2018-06697
http://www.cnvd.org.cn/flaw/show/CNVD-2018-06698
http://www.cnvd.org.cn/flaw/show/CNVD-2018-06699
http://www.cnvd.org.cn/flaw/show/CNVD-2018-06700
http://www.cnvd.org.cn/flaw/show/CNVD-2018-06313

4、Linux 产品安全漏洞

Linux kernel 是美国 Linux 基金会发布的操作系统 Linux 所使用的内核。本周，该

产品被披露存在拒绝服务漏洞，攻击者可利用漏洞发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Linux kernel 拒绝服务漏洞（CNVD-2018-06306、CNVD-2018-06440、CNVD-2018-06300、CNVD-2018-06401、CNVD-2018-06431、CNVD-2018-06432、CNVD-2018-06459、CNVD-2018-06460）。其中“Linux kernel 拒绝服务漏洞（CNVD-2018-06306、CNVD-2018-06440）”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-2018-06306
http://www.cnvd.org.cn/flaw/show/CNVD-2018-06440
http://www.cnvd.org.cn/flaw/show/CNVD-2018-06300
http://www.cnvd.org.cn/flaw/show/CNVD-2018-06401
http://www.cnvd.org.cn/flaw/show/CNVD-2018-06431
http://www.cnvd.org.cn/flaw/show/CNVD-2018-06432
http://www.cnvd.org.cn/flaw/show/CNVD-2018-06459
http://www.cnvd.org.cn/flaw/show/CNVD-2018-06460

5、Tenda AC15 路由器代码执行漏洞

Tenda AC15 router 是中国腾达（Tenda）公司的一款无线路由器产品。本周，Tenda 被披露存在权限获取漏洞，远程攻击者可借助特制的‘COOKIE’参数利用该漏洞执行代码。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-2018-06266

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-2018-06237	Joomla! Saxum Astro 组件 SQL 注入漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：http://www.saxum2003.hu/
CNVD-2018-06238	Joomla! SquadManagement 组件 SQL 注入漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：http://www.larshildebrandt.de/
CNVD-2018-06239	Joomla! Saxum Numerology 组件 SQL 注入漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：http://www.saxum2003.hu/
CNVD-2018-06287	Invision Power Services Invision Power Board SQL 注入漏洞	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://invisioncommunity.com/
CNVD-201	PureVPN Windows 权限提升	高	厂商已发布漏洞修复程序，请及时关

8-06301	漏洞		注更新：https://www.purevpn.com/
CNVD-2018-06426	Icinga 任意代码执行漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://github.com/Icinga/icinga2/pull/5850
CNVD-2018-06465	GLPI 远程代码执行漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://github.com/glpi-project/glpi/pull/3650
CNVD-2018-06512	LepideAuditor Suite 'genratereports.php'命令注入漏洞	高	用户可联系供应商获得补丁信息：https://www.lepide.com/lepideauditor/
CNVD-2018-06557	Citrix NetScaler ADC 和 NetScaler Gateway 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://support.citrix.com/article/CTX232161
CNVD-2018-06559	CactusVPN root 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://www.cactusvpn.com/

小结：本周，Drupal 被披露存在远程代码执行漏洞，攻击者可利用漏洞执行任意代码。此外，Google、Microsoft、Linux 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、提升权限或发起拒绝服务攻击等。另外，Tenda 被披露存在权限获取漏洞，远程攻击者可借助特制的‘COOKIE’参数利用该漏洞执行代码。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. 罗克韦尔 MicroLogix-1400-PLC 曝多个高危漏洞

思科 Talos 团队 3 月 28 日发博文指出，罗克韦尔 Allen-Bradley MicroLogix 1400 可编程逻辑控制器（PLC）中存在多个严重的漏洞，这些漏洞可用来发起 DoS 攻击，修改设备的配置和梯形逻辑，写入或删除其内存模块上的数据。罗克韦尔已发布固件更新来解决其中部分漏洞，并提出了一系列缓解措施，例如将开关设置为“Hard Run”即可防止未经授权的更改行为，并禁用受影响的服务。

参考链接：https://www.easyaq.com/news/1829645244.shtml

2. 思科爆重大远端程式码执行漏洞

思科于上周六发布的 IOS 及 IOS XE 软件安全公告中，被认为潜在威胁最大的漏洞被标识为 CVE-2018-0171，可能会威胁到到超过数百万台网络设备（主要是路由器和交换机）的安全。来自俄罗斯安全公司 Embedi 的安全研究员 George Nosenko 在 IOS 和 I

OS-XE 系统 Smart Install Client 代码中发现了这个缓冲区堆栈溢出漏洞。成功利用这个漏洞可允许攻击者对设备发起拒绝服务（DoS）攻击，或在未经身份验证的情况下远程执行任意代码，这意味着攻击者可以通过利用这个漏洞来获得对受影响设备的完全控制权限。

参考链接：https://www.easyaq.com/news/887520524.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