

信息安全漏洞周报

2016 年 04 月 25 日-2016 年 05 月 01 日

2016年第18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 191 个，其中高危漏洞 46 个、中危漏洞 112 个、低危漏洞 33 个。漏洞平均分为 5.54 分。本周收录的漏洞中，涉及 0day 漏洞 17 个（占 9%）。其中互联网上出现“Advanced Electron Forum 跨站脚本漏洞、WordPress Booking Calendar Contact Form 插件 SQL 注入漏洞”等零日代码攻击漏洞，请使用相关产品的用户注意加强防范。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 1604 个，与上周（869 个）环比增长 85%。此外，由于 Apache Struts 2 S2-032 远程代码执行漏洞利用代码的披露，导致事件型漏洞数量以及针对互联网站的大规模攻击威胁增加，本周安全威胁级别调整为“高”。

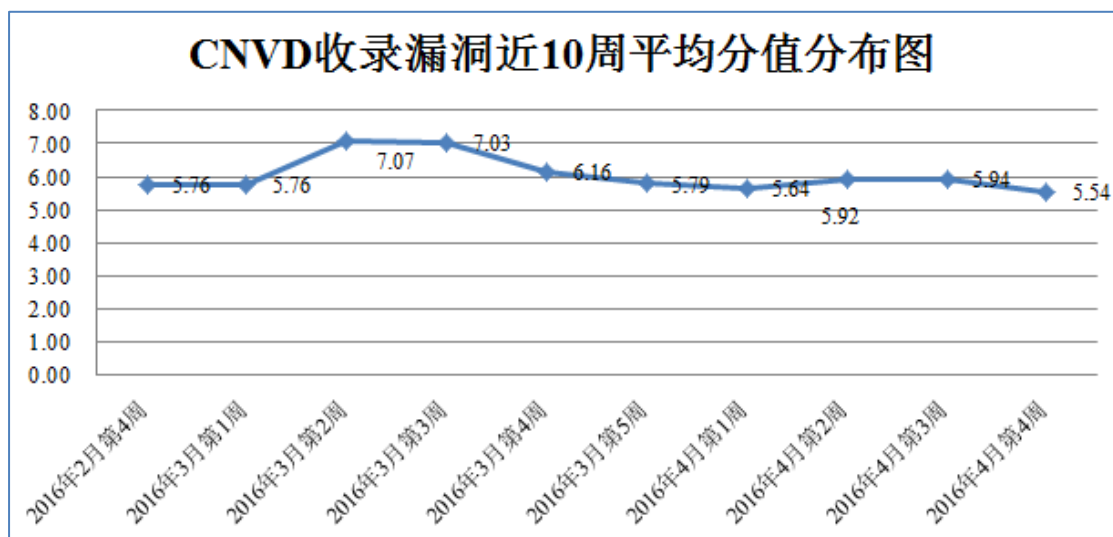


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周，共 9 家成员单位、合作伙伴及个人报送了本周收录的全部 191 个漏洞。报送

情况如表 1 所示。其中，天融信、绿盟科技、安天实验室等单位报送数量较多。补天平台、乌云、漏洞盒子、上海云盾信息技术有限公司 High-TechBridge Security Research Lab 及白帽子向 CNVD 提交了 1604 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
奇虎(补天平台)	981	981
天融信	191	0
绿盟科技	178	0
安天实验室	133	0
启明星辰	82	1
杭州安恒信息技术有限公司	60	0
恒安嘉新	29	6
H3C	6	0
东软	244	0
乌云	417	417
漏洞盒子	126	126
上海云盾信息技术有限公司	5	5
CNCERT 江西分中心	8	8
CNCERT 安徽分中心	4	4
CNCERT 福建分中心	1	1
CNCERT 云南分中心	1	1
CNCERT 甘肃分中心	1	1
High-Tech Bridge Security Research Lab	1	1
个人	52	52
报送总计	2520	1604

录入总计	191（去重）	1604
------	---------	------

表 1 成员单位上报漏洞统计表

本周漏洞按类型和厂商统计

本周，CNVD 收录了 191 个漏洞。其中应用程序漏洞 116 个，数据库漏洞 30 个，操作系统漏洞 20 个，Web 应用漏洞 13 个，网络设备漏洞 12 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	116
数据库漏洞	30
操作系统漏洞	20
web 应用漏洞	13
网络设备漏洞	12

表 2 漏洞按影响类型统计表

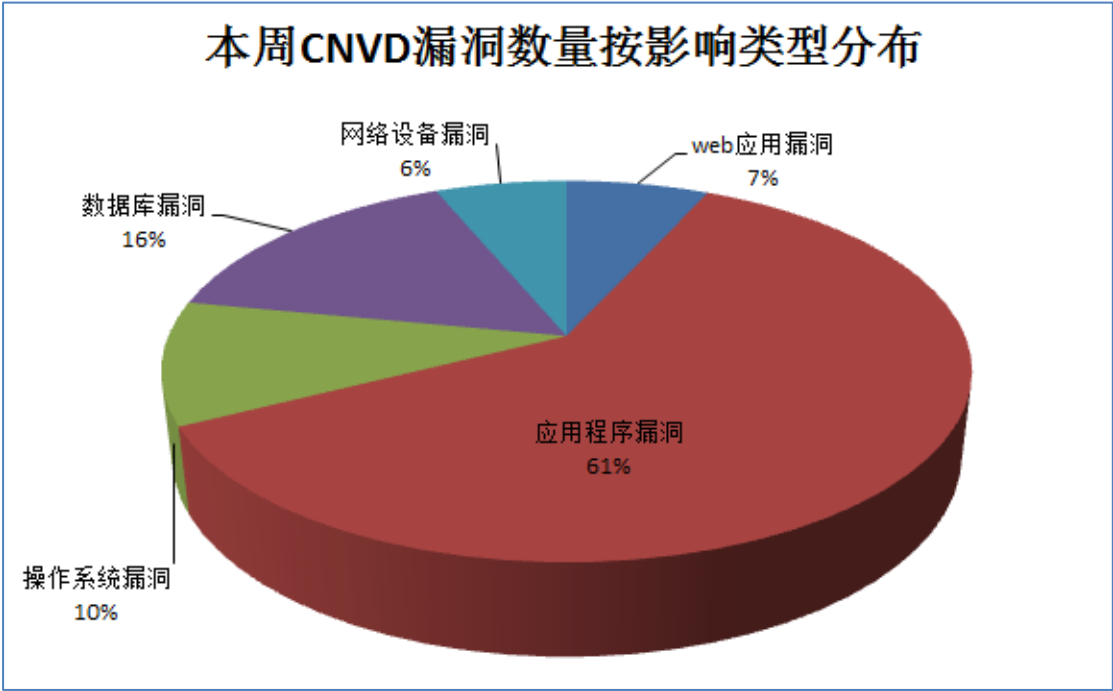


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、Joyent、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。

序号	厂商（产品）	漏洞数量	所占比例
1	Oracle	81	42%
2	Joyent	16	8%
3	Wireshark	11	6%

4	Linux	11	6%
5	PHP	4	2%
6	Squid	4	2%
7	Cisco	4	2%
8	IBM	3	2%
9	Plone	3	2%
10	其他	54	28%

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 47 个电信行业漏洞、5 个移动互联网漏洞（如下图所示）。其中，“SystechSysLINK M2M Modular Gateway 权限获取漏洞、SystechSysLINK M2M Modular Gateway 命令执行漏洞、Oracle MySQL Server:Pluggable Authentication 子组件存在未明漏洞、AVM FRITZ!Boxh 栈缓冲区溢出漏洞、Oracle Database Server Java V M 组件存在未明漏洞、Oracle Database Server OLAP 组件存在未明漏洞、Cisco Wireless LAN Controller Web 管理接口拒绝服务漏洞、Oracle Fusion Middleware WebLogic Server 组件存在未明漏洞（CNVD-2016-02575、CNVD-2016-02481）、Cisco Wireless LAN Controller 拒绝服务漏洞（CNVD-2016-02518、CNVD-2016-02517）、Samsung android phone v4l-subdev 驱动程序内存破坏漏洞、BlackBerry Enterprise Service 管理控制台 SQL 注入漏洞”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/>

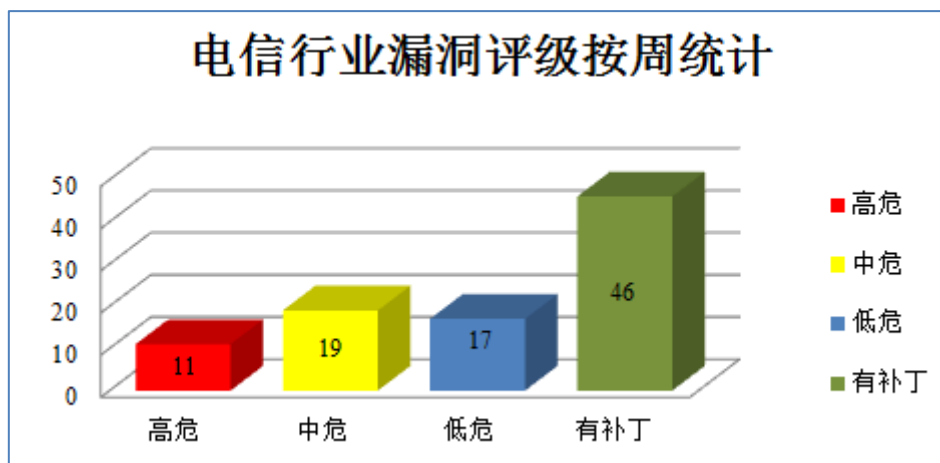


图 3 电信行业漏洞统计

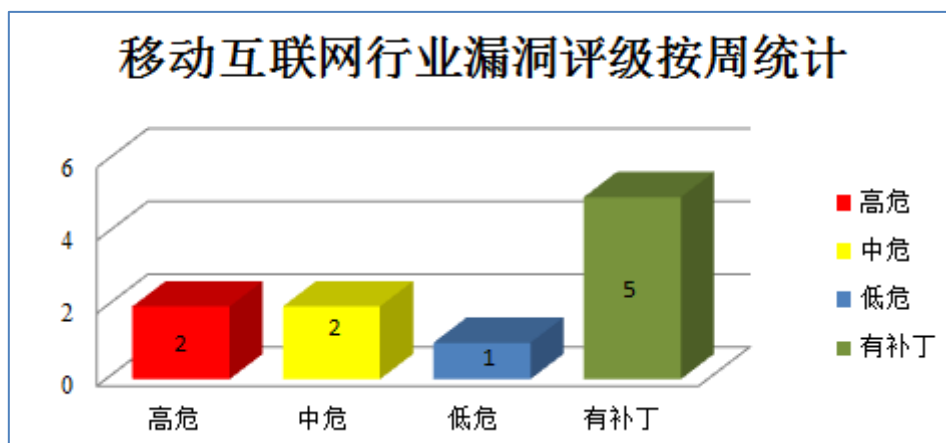


图 4 移动互联网行业漏洞统计

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、Apache Struts2 产品安全漏洞

本周，互联网上披露了 Apache Struts 2 S2-032 远程代码执行漏洞（CNVD-2016-02506，CVE-2016-3081）的利用代码，根据 CNVD 初步测试，远程攻击者利用漏洞可在开启动态方法调用功能的 Apache Struts 2 服务器上执行任意代码，取得网站服务器控制权。

CNVD 收录的相关漏洞包括：Apache Struts XSLTResult 任意代码执行漏洞、Apache Struts2 远程代码执行漏洞（CNVD-2016-02506）。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-2016-02662>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-02506>

2、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，该产品被披露存在缓冲区溢出和拒绝服务漏洞，允许攻击者利用漏洞发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Linux kernel ext4 组件拒绝服务漏洞、Linux kernel AIO Interface 组件缓冲区溢出漏洞、Linux kernel CUSE Driver 组件拒绝服务漏洞、Linux kernel snd-usb-audio Driver 组件拒绝服务漏洞、Linux kernel PowermateDriver 组件拒绝服务漏洞、Linux kernel iowarrior Driver 组件拒绝服务漏洞、Linux kernel ati_remote2 Driver 组件拒绝服务漏洞、Linux kernel 拒绝服务漏洞（CNVD-2016-02592）等。

目前，厂商已经发布了上述漏洞中除“Linux kernel snd-usb-audio Driver 组件拒绝服务漏洞、Linux kernel PowermateDriver 组件拒绝服务漏洞、Linux kernel iowarrior Driver 组件拒绝服务漏洞、Linux kernel ati_remote2 Driver 组件拒绝服务漏洞”外，其余漏洞的修补程序。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-2016-02604>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-02591>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-02590>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-02589>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-02588>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-02587>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-02586>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-02592>

3、Wireshark 产品安全漏洞

Wireshark（前称 Ethereal）是 Wireshark 团队开发的一套网络数据包分析软件。本周，上述产品被披露存在拒绝服务漏洞，允许攻击者利用漏洞发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Wireshark PKTC 解析器拒绝服务漏洞、Wireshark I AX2 解析器拒绝服务漏洞、Wireshark GSM CBCH 解析器拒绝服务漏洞、WiresharkTS hark 拒绝服务漏洞、Wireshark 拒绝服务漏洞（CNVD-2016-02664）、Wireshark NCP 解析器拒绝服务漏洞（CNVD-2016-02649）、Wireshark PKTC 解析器拒绝服务漏洞（CNVD-2016-02651）、Wireshark MS-WSP 解析器拒绝服务漏洞（CNVD-2016-02654）等。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-2016-02650>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-02652>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-02653>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-02657>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-02664>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-02649>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-02651>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-02654>

4、Cisco 产品安全漏洞

Cisco ASA 5500 系列自适应安全设备是用于提供安全和 VPN 服务的模块化平台，可提供防火墙、IPS、anti-X 和 VPN 服务。Cisco WLC 负责全系统的无线 LAN 功能，例如安全策略、入侵保护、RF 管理，服务质量和移动性。本周，上述产品被披露存在拒绝服务漏洞，允许攻击者利用漏洞发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco Adaptive Security Appliance Software DHCPv6 中继拒绝服务漏洞、Cisco Wireless LAN Controller Web 管理接口拒绝服务漏洞、Cisco Wireless LAN Controller 拒绝服务漏洞（CNVD-2016-02518、CNVD-2016-02517）。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-2016-02520>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-02519>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-02518>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-02517>

5、WordPress Booking Calendar Contact Form 插件 SQL 注入漏洞（CNVD-2016-02465）

WordPress 是 WordPress 软件基金会的一套使用 PHP 语言开发的博客平台，该平台支持在 PHP 和 MySQL 的服务器上架设个人博客网站。本周，WordPress Booking Calendar Contact Form 插件被披露存在 SQL 注入漏洞，允许攻击者利用漏洞执行未经授权数据库操作。目前，互联网上已经出现了针对该漏洞的攻击代码，厂商尚未发布该漏洞的修补程序。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-2016-02465>

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-2016-02505	PHPback 'orderby'参数 SQL 注入漏洞	高	目前厂商已发布了新版本修复该漏洞，请将软件更新至 3.1.3 版本： https://github.com/ivandiazwm/phpback/releases
CNVD-2016-02521	HPE P9000 CVAE 任意命令执行漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05085438
CNVD-2016-02513	NetBSDbozohttpd CGI 处理器任意代码执行漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： http://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2016-005.txt.asc
CNVD-2016-02537	IBM Spectrum Scale 敏感信息泄露漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： https://www-304.ibm.com/support/docview.wss?uid=ssg1S1005742

CNVD-2016-02540	Joyent Node.js handlebar 命令注入漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： https://nodesecurity.io/advisories/61
CNVD-2016-02541	Joyent Node.js mustache 命令注入漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： https://nodesecurity.io/advisories/62
CNVD-2016-02597	Plone 权限提升漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： https://plone.org/security/20160419/privilege-escalation-in-webdav
CNVD-2016-02620	modified eCommerce 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.modified-shop.org/
CNVD-2016-02631	Tenable Network Security Tenable Nessus Mac OS X Scanning 组件权限提升漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： http://www.tenable.com/security/tns-2016-02
CNVD-2016-02625	AVM FRITZ!Boxh 栈缓冲区溢出漏洞	高	用户可联系供应商获得补丁信息： http://avm.de/

表 4 部分重要高危漏洞列表

小结：互联网上披露了 Apache Struts 2 S2-032 远程代码执行漏洞（CNVD-2016-02506，CVE-2016-3081）的利用代码，根据 CNVD 初步测试，远程攻击者利用漏洞可在开启动态方法调用功能的 Apache Struts 2 服务器上执行任意代码，取得网站服务器控制权。此外，Linux、Wireshark、Cisco 等多款产品被披露存在多个安全漏洞，攻击者利用漏洞可发起拒绝服务攻击等。另外，WordPress Booking Calendar Contact Form 插件被披露存在一个高危漏洞，允许攻击者利用漏洞执行未授权数据库操作。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. 思科发现一千两百万台 PC 存在后门间谍程序

思科 Talos Group 的安全研究人员表示：法国 Tuto4PC 公司悄悄在 PC 上绑定广告软件和间谍软件。该法国公司的其他一些工具，包括 OneSoftPerDay 和 System Healer 等，都存在恶意行为的木马。一旦电脑用户安装 Tuto4PC 的任何一种实用程序，该软件就会运行恶意程序并安装名为“Wizz”的木马程序。Wizz 有管理权限，不仅能下载和安装其它程序，还能收集个人信息、安装并运行控制方上传的可执行文件等。

参考链接：<http://www.freebuf.com/news/103203.html>

2. 卡塔尔国家银行被黑，1.4G 数据泄露

匿名黑客组织宣布攻破了卡塔尔国家银行系统，并在 Cryptome 网站上公开了从卡

卡塔尔国家银行(Qatar National Bank)窃取容量超过 1.4GB 的数据转储文件。数据包含该银行客户资料、密码、PIN 码、支付卡数据、家庭住址、电子邮件和其他 PII（个人识别资料）数据等。此外，黑客还宣称窃取了卡塔尔王室 Al-Thani 以及卡塔尔 Al Jazeera 电视台记者的银行信息。访问过该泄露数据库的人都会被泄露数据中的一个标记为“间谍”的文件夹所吸引。浏览后发现，该文件里面包含了卡塔尔王室数据，卡塔尔国防部和各种情报机构信息，甚至涉及英国(军情六处)，法国和波兰等国情报信息。

参考链接: <http://www.freebuf.com/news/102939.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