

信息安全漏洞周报

2016 年 09 月 05 日-2016 年 09 月 09 日

2016 年第 37 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 20 个，其中高危漏洞 116 个、中危漏洞 91 个、低危漏洞 13 个。漏洞平均分为 6.52。本周收录的漏洞中，涉及 0day 漏洞 132 个（占 60%）。其中互联网上出现“ZKTeco ZKTime.Net 不安全文件权限提升漏洞、ArcServe UDP 服务器路径权限提升漏洞”零日代码攻击漏洞，请使用相关产品的用户注意加强防范。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 968 个，与上周（1107 个）环比下降 12%。

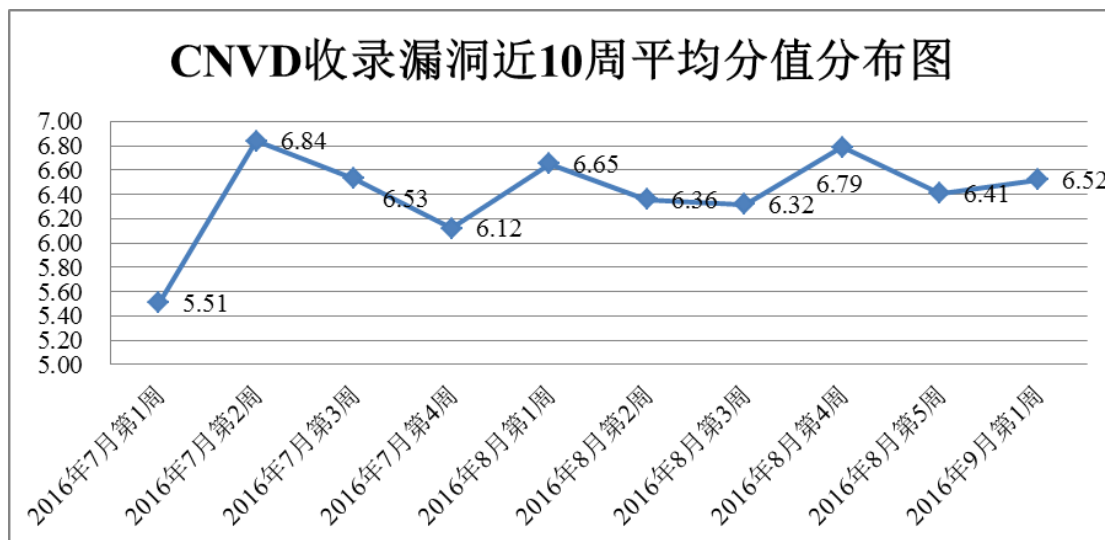


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周，共 10 家成员单位、合作伙伴及企业用户、个人用户报送了本周收录的全部 20 个漏洞。报送情况如表 1 所示。其中，安天实验室、启明星辰、恒安嘉新、H3C 等单位报送数量较多。奇虎（补天平台）、漏洞盒子、深圳市深信服电子科技有限公司、北京安信天行科技有限公司、腾讯玄武实验室、西安四叶草信息技术有限公司、广州神

月信息安全技术有限公司、新疆天山智汇信息科技有限公司、中国航天科工四院软件评测中心及其他个人白帽子向 CNVD 提交了 968 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）	923	923
安天实验室	122	0
启明星辰	120	0
恒安嘉新	104	1
H3C	77	0
天融信	68	0
东软	43	0
杭州安恒信息技术有限公司	31	0
绿盟科技	30	0
中国电信集团系统集成有限责任公司	21	0
漏洞盒子	20	0
深圳市深信服电子科技有限公司	10	10
北京安信天行科技有限公司	5	5
腾讯玄武实验室	5	5
西安四叶草信息技术有限公司	3	3
广州神月信息安全技术有限公司	2	2
新疆天山智汇信息科技有限公司	1	1
中国航天科工四院软件评测中心	1	1
CNCERT 新疆分中心	3	3
CNCERT 宁夏分中心	2	2

个人	12	12
报送总计	1603	968
录入总计	220（去重）	968

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 220 个漏洞。其中 web 应用漏洞 110 个，应用程序漏洞 89 个，安全产品 9 个，网络设备漏洞 6 个，操作系统漏洞 4 个，数据库漏洞 2 个。

漏洞影响对象类型	漏洞数量
web 应用漏洞	110
应用程序漏洞	89
安全产品漏洞	9
网络设备漏洞	6
操作系统漏洞	4
数据库漏洞	2

表 2 漏洞按影响类型统计表

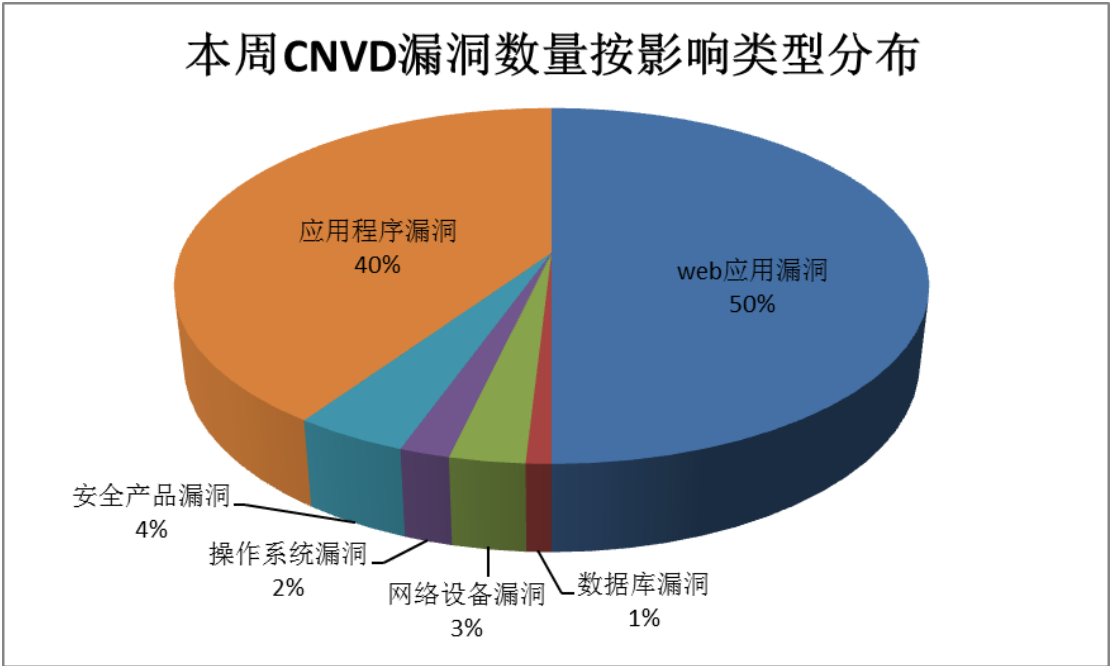


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、PHP、zzcms 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	Google	23	10%

2	PHP	17	8%
3	zzcms	10	5%
4	Red Hat	7	3%
5	Plone	6	3%
6	Fortinet	5	2%
7	QEMU	4	2%
8	Siemens	3	1%
9	OpenSSL	2	1%
10	其他	143	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 3 个电信行业漏洞，4 个移动互联网行业漏洞（如下图所示）。详情请参照 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/>

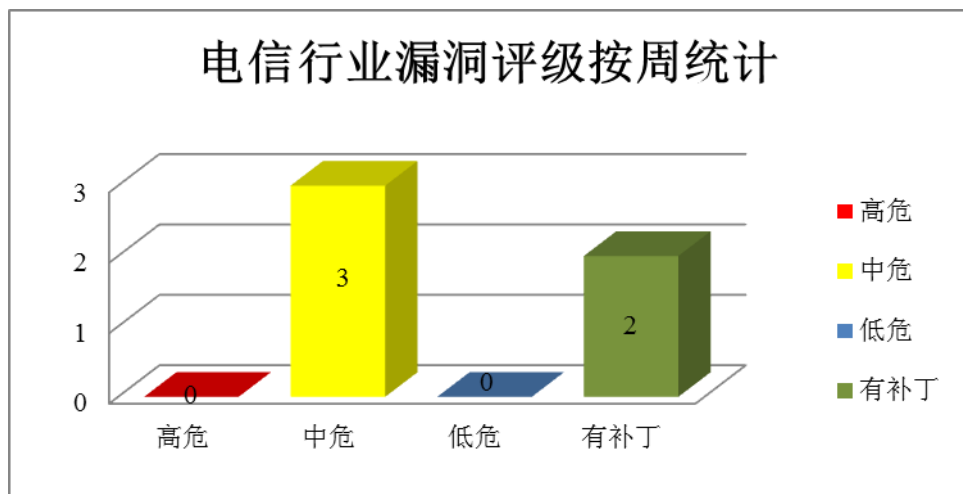


图 3 电信行业漏洞统计

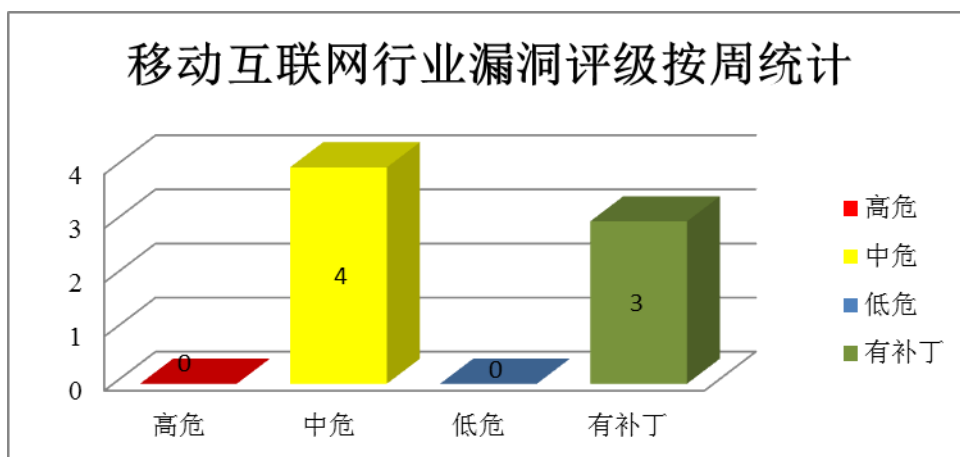


图 4 移动互联网行业漏洞统计

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、Google 产品安全漏洞

Google Chrome 是美国谷歌（Google）公司开发的一款 Web 浏览器。PDFium 是其中的一个开源 PDF 渲染引擎。本周，上述产品被披露存在堆缓冲区溢出和任意代码执行漏洞，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 Chrome PDFium 堆缓冲区溢出漏洞（CNVD-2016-07196、CNVD-2016-07197、CNVD-2016-07206、CNVD-2016-07207）、Google Chrome 任意代码执行漏洞（CNVD-2016-07195、CNVD-2016-07209、CNVD-2016-07210、CNVD-2016-07215）等。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-2016-07196>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07197>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07206>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07207>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07195>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07209>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07210>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07215>

2、PHP 产品安全漏洞

PHP 是一种开源的通用计算机脚本语言。本周，该产品被披露存在本地拒绝服务漏洞，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：PHP 5.0.0 'fbird_[p]connect()'本地拒绝服务漏洞、PH

P 5.0.0 'snmprealwalk()'本地拒绝服务漏洞、PHP 5.0.0 'snmpset()'本地拒绝服务漏洞、PHP 5.0.0 'snmpwalk()'本地拒绝服务漏洞、PHP 5.0.0 'snmpwalkoid()'本地拒绝服务漏洞、PHP 5.0.0 'xmldocfile()' 本地拒绝服务漏洞、PHP 'AppendIterator::append'本地拒绝服务漏洞、PHP JsonSerializable::jsonSerialize json_encode 本地拒绝服务漏洞等。目前，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-2016-07222>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07220>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07223>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07221>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07219>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07224>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07399>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07400>

3、Zzcms 产品安全漏洞

ZZCMS 突出招商及供求功能，可快速搭建产品招商网站。本周，该产品被披露存在 SQL 注入漏洞，攻击者可利用漏洞获取数据库敏感数据。

CNVD 收录的相关漏洞包括：zzcms 最新产品版/zx/search.php 页面存在 SQL 注入漏洞、zzcms 最新产品版/zs/search.php 页面存在 SQL 注入漏洞、zzcms 存在 SQL 盲注漏洞、zzcms zs/contrast.php 存在 SQL 注入漏洞、zzcms user/del.php 存在 SQL 注入漏洞、zzcms inc/stopsqlin.php 存在 SQL 注入漏洞、zzcms 最新产品版/pp/search.php 页面存在 SQL 注入漏洞、zzcms /dl/show.php 存在 SQL 注入漏洞等。上述漏洞的综合评级为“高危”。目前，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-2016-07227>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07228>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07186>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07188>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07189>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07190>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07191>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07193>

4、Red Hat 产品安全漏洞

Red Hat OpenShift 是美国红帽（Red Hat）公司的一款平台即服务（PaaS）云计算平台。OpenShift Enterprise 是一个开源的私有云版本。Red Hat JBoss BPMS 是一套集

合了 JBoss BRMS 所有功能的业务流程管理平台。Red Hat oVirt Engine 是一套开源的虚拟化管理平台。RESTEasy 是 JBoss 的开源项目之一，是一个 RESTful Web Services 框架。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞泄露敏感信息或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Red Hat OpenShift Enterprise 拒绝服务漏洞、Red Hat OpenShift Enterprise 拒绝服务漏洞（CNVD-2016-07357）、Red Hat JBoss BPMS 存在多个 HTML 注入漏洞、Red Hat JBoss BPMS 跨站请求伪造漏洞、Red Hat oVirt Engine 本地信息泄露漏洞、Red Hat RESTEasy 信息泄露漏洞、Red Hat RESTEasy 拒绝服务漏洞。目前，厂商已经发布了“Red Hat OpenShift Enterprise 拒绝服务漏洞、Red Hat OpenShift Enterprise 拒绝服务漏洞（CNVD-2016-07357）”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-2016-07356>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07357>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07326>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07325>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07270>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07272>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07273>

5、ArcServe UDP 服务器路径权限提升漏洞

Arcserve UDP 是一套统一数据保护解决方案。本周，Arcserve UDP 被披露存在权限提升漏洞。攻击者可利用漏洞在搜索路径目录放置一个恶意的二进制和提升权限。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-2016-07398>

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-2016-07188	zzcms zs/contrast.php 存在 SQL 注入漏洞	高	暂无
CNVD-2016-07189	zzcms user/del.php 存在 SQL 注入漏洞	高	暂无
CNVD-2016-07190	zzcms inc/stopsqlin.php 存在 SQL 注入漏洞	高	暂无
CNVD-2016-07218	ZKTeco ZKTime.Net 不安全文件权限提升漏洞	高	暂无
CNVD-2016-07339	Fortinet FortiWAN 命令注入漏洞	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://docs.fortinet.com/uploaded/files/3236/fortiwan-v4.2.5-release-notes.pdf
CNVD-2016-07338	Zoomla!CMS 最新版文件上传漏洞	高	暂无
CNVD-2016-07351	Dentsply Sirona CDR DICOM 硬编码凭证安全绕过漏洞	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://www.schickbysirona.com/items.php?catid=714
CNVD-2016-07345	Open Dental 硬编码凭证安全绕过漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页： http://www.opendental.com/manual/mysql.html
CNVD-2016-07398	ArcServe UDP 服务器路径权限提升漏洞	高	暂无
CNVD-2016-07403	DEXIS Imaging Suite 硬编码凭证漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息： http://www.kb.cert.org/vuls/id/282991

表 4 部分重要高危漏洞列表

小结：本周，Google 产品被披露存在堆缓冲区溢出和任意代码执行漏洞，攻击者可利用漏洞执行任意代码。此外，PHP、Zcms、Red Hat 等多款产品被披露存在多个安全漏洞，攻击者可利用漏洞获取数据库敏感数据或发起拒绝服务攻击等。另外，Arcserve UDP 被披露存在权限提升漏洞。攻击者可利用漏洞在搜索路径目录放置一个恶意的二进制和提升权限。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. BlackHat 议题解析：Windows 程序的数字签名校验“漏洞”

在今年的黑帽大会上，国外的一个安全研究员展示了如何通过 Windows 的数字签名 bypass 对恶意程序代码的检测。下载大会的该演讲的 ppt 大概看了一下，报告分为两部分，第一部分展示数字签名的校验“漏洞”，第二部分展示该作者自己研究实现的一个 pe 程序加载器，用来配合第一部分的“漏洞”bypass 杀毒软件对恶意程序的检测。实际上这个程序签名的“漏洞”并算不上通常意义上的漏洞，但是却因为本身比较容易被概念混淆，使用可能没有充分得当，导致可能存在一些比较严重的可利用环节。所以，程序的数字签名只能用于验证程序的代码和数据是否被篡改，而无法用于验证程序文件本身是否被篡改。

参考链接：<http://www.freebuf.com/vuls/113527.html>

2. 关于爱快 iKuai 路由产品漏洞情况的通报

近日，国家信息安全漏洞库（CNNVD）收到北京长亭科技有限公司关于企业级流路由产品“iKuai IK-G20SQL 注入漏洞”，“iKuai 小白 SQL 注入漏洞”和“iKuai 小白命令注入漏洞”的情况报送。上述漏洞均由于未对用户输入进行有效验证，导致远程攻击者可利用该漏洞对使用受影响产品进行远程攻击。由于该漏洞影响范围较广，危害较为严重，根据 CNNVD 相关规定，已对此漏洞进行收录，并分配编号 CNNVD-201608-553、CNNVD-201608-554、CNNVD-201608-555。经 CNNVD 与厂商沟通确认，“iKuai IK-G20”和“iKuai 小白”将于下一版本发布漏洞补丁，请可能受影响的用户及时关注信息。在此之前，使用上述设备的用户，经厂商确认可使用如下临时解决方案：（1）针对“iKuaiIK-G20”路由产品，可通过关闭 telnet 登录消除安全隐患。（2）修改 iKuai 路由产品密码为复杂口令，避免弱口令。。

参考链接：<http://www.freebuf.com/news/114047.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