

信息安全漏洞周报

2015 年 05 月 18 日-2015 年 05 月 24 日

2015 年第 21 期

本周漏洞基本情况

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 182 个，其中高危漏洞 62 个、中危漏洞 112 个、低危漏洞 8 个。上述漏洞中，可利用来实施远程攻击的漏洞有 172 个。本周收录的漏洞中，已有 152 个漏洞由厂商提供了修补方案，建议用户及时下载补丁更新程序，避免遭受网络攻击。其中互联网上出现“ProjectSend 任意文件上传漏洞”等零日攻击代码，请使用相关产品的用户注意加强防范。

成员单位报送漏洞统计

本周，共 6 家成员单位、合作伙伴及个人报送了本周收录的全部 182 个漏洞。报送情况如表 1 所示。其中，奇虎、绿盟科技、启明星辰、天融信等单位报送数量较多。此外，CNCERT 各分中心、乌云、漏洞盒子、上海天泰网络技术有限公司、汉柏科技有限公司及白帽子向 CNVD 提交了 902 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	565	565
绿盟科技	147	0
启明星辰	132	0
天融信	101	0
安天实验室	88	0
恒安嘉新	37	0

High-Tech Bridge Security Research Lab	1	1
乌云	280	280
漏洞盒子	30	30
上海天泰网络技术有限公司	1	1
汉柏科技有限公司	1	1
CNCERT 宁夏分中心	2	2
个人	22	22
报送总计	1407	902
录入总计	182（去重）	902

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Adobe、Drupal、Cisco 等多家厂商的产品，部分漏洞数量按厂商统计如表 2 所示。

序号	厂商（产品）	漏洞数量	所占比例
1	Adobe	39	21%
2	Drupal	16	9%
3	Cisco	16	9%
4	WordPress	12	7%
5	Wireshark	8	4%
6	IBM	6	3%
7	Mozilla	5	3%
8	SAP	4	2%
9	Amazon	3	2%
10	其他	73	40%

表 2 漏洞产品涉及厂商分布统计表

漏洞按影响类型统计

本周，CNVD 收录了 182 个漏洞。其中应用程序漏洞 128 个，WEB 应用漏洞 36 个，网络设备漏洞 7 个，操作系统漏洞 5 个，安全产品漏洞 5 个，数据库漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	128
WEB 应用漏洞	36
网络设备漏洞	7
操作系统漏洞	5
安全产品漏洞	5
数据库漏洞	1

表 3 漏洞按影响类型统计表

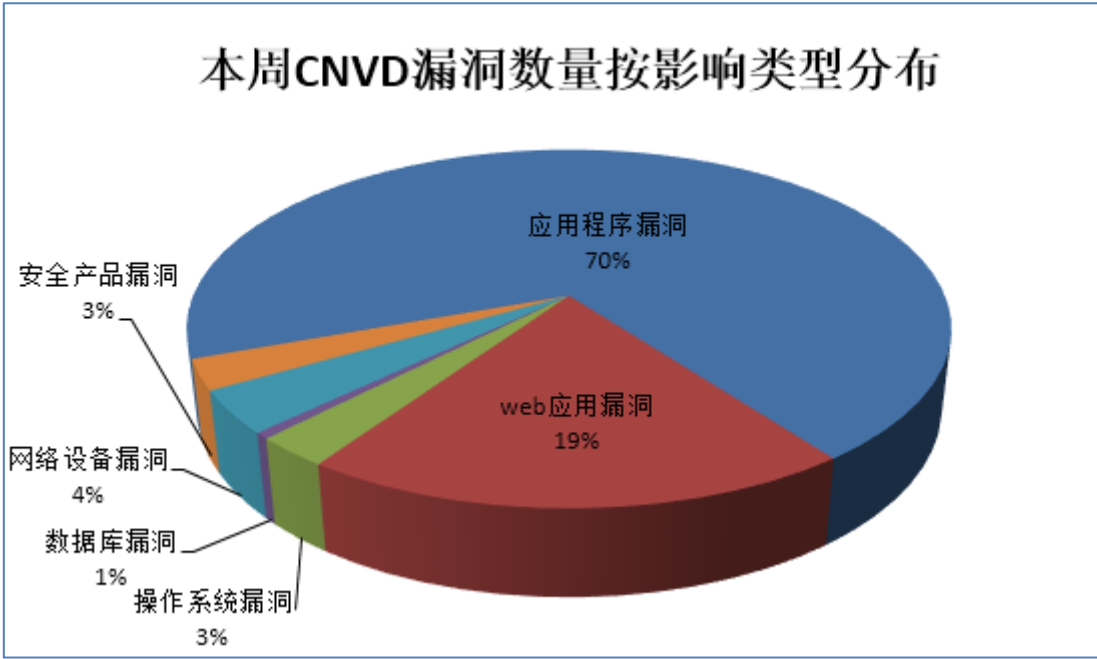


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 6 个电信行业漏洞（如下图表所示）。其中，“EFMNetworks ipTIME CGI 文件处理远程代码执行漏洞”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。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2015-03231	Cisco Wireless LAN Controller 拒绝服务漏洞（CNVD-2015-03231）	中	是
电信	CNVD-2015-03242	Cisco WebEx Meetings Server 存在多个跨站脚本漏洞	中	是
电信	CNVD-2015-03261	PostgreSQL 不安全哈希密码漏洞	中	否
电信	CNVD-2015-03273	Cisco IOS ISDN 实现拒绝服务漏洞	中	是
电信	CNVD-2015-03310	IBM WebSphere Commerce 本地信息泄露漏洞	低	是
电信	CNVD-2015-03297	EFMNetworks ipTIME CGI 文件处理远	高	是

		程代码执行漏洞		
--	--	---------	--	--

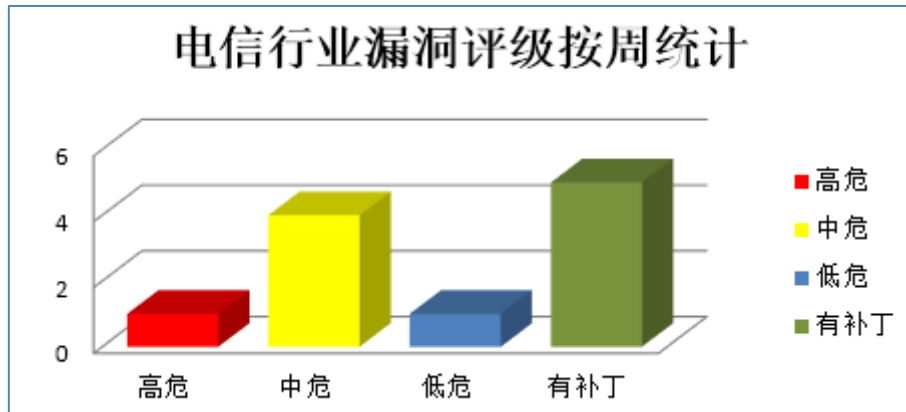


图 1 电信行业漏洞统计

本周重要漏洞信息

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

Adobe Reader/Acrobat 是流行的处理 PDF 文件的应用程序。本周，上述产品被披露存在未明内存破坏任意代码执行漏洞。攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Reader/Acrobat 存在未明内存破坏任意代码执行漏洞（CNVD-2015-03140、CNVD-2015-03139、CNVD-2015-03132、CNVD-2015-03133、CNVD-2015-03134、CNVD-2015-03135、CNVD-2015-03137、CNVD-2015-03138）。上述漏洞的综合评级均为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户尽快下载补丁更新，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-2015-03140>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03139>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03132>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03133>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03134>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03135>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03137>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03138>

2、Cisco 产品安全漏洞

Cisco TelePresence 是思科公司开发的网真会议解决方案。Cisco Adaptive Security Appliance 是一款自适应安全设备，可提供安全和 VPN 服务的模块。Cisco MediaSense 提供录像，回放，流媒体直播，和存储媒体，包括音频和视频，以改善客户服务。Cisco Unified Intelligence Center 是美国思科（Cisco）公司的一套基于 Web 的报表平台。该平

台提供报告相关的业务数据和呼叫中心数据的全面展示等功能。Cisco Secure Access Control System 是访问策略控制平台。Cisco WebEx Meetings Server 是一款思科公司推出的思科会议中心实现。本周，上述产品被披露存在多个安全漏洞。攻击者可利用漏洞获取敏感信息，提升权限、执行跨站脚本、跨站请求伪造攻击或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco TelePresence 高速 IP 报文处理拒绝服务漏洞、Cisco TelePresence 验证绕过权限提升漏洞、Cisco TelePresence 多个产品远程命令注入漏洞、Cisco Web Security Appliance 存在未明跨站脚本漏洞、Cisco MediaSense 跨站请求伪造漏洞、Cisco Unified Intelligence Center 跨站请求伪造漏洞、Cisco Access Control Server 文件包含漏洞、Cisco WebEx Meetings Server 存在多个跨站脚本漏洞。其中，“Cisco TelePresence 高速 IP 报文处理拒绝服务漏洞、Cisco TelePresence 验证绕过权限提升漏洞、Cisco TelePresence 多个产品远程命令注入漏洞”的综合评级均为“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-2015-03238>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03239>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03234>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03276>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03271>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03246>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03241>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03242>

3、IBM 产品安全漏洞

IBM SPSS Statistics 是一套统计分析软件，它能够帮助企业解决从计划和数据收集到分析、报告和部署的整个分析过程中的问题。IBM Bluemix 是一套用于建设、运行和管理应用程序和服务的云平台。IBM InfoSphere Optim Workload Replay 是美国 IBM 公司的一套用于重放真实的数据库生产活动并提供变更影响报告、快速地发现问题的解决方案。IBM WebSphere Commerce 是业界领先的下一代电子商务解决方案。IBM Tivoli Netcool Service Quality Manager 是一套将服务质量管理和服务水平协议组合用来管理电信服务质量的解决方案。IBM PureApplication System 是一套专为事务性 Web 和数据库应用程序而设计的平台系统。本周，上述产品被披露存在信息泄露、跨站请求伪造和远程代码执行漏洞。攻击者可利用漏洞获取敏感信息、进行跨站请求伪造攻击或执行任意代码。

CNVD 收录的相关漏洞包括：IBM SPSS Statistics ActiveX 控件代码执行漏洞、IBM Workflow for Bluemix 信息泄露漏洞、IBM InfoSphere Optim Workload Replay 跨站请求伪造漏洞、IBM WebSphere Commerce 本地信息泄露漏洞、IBM Tivoli Netcool

Service Quality Manager 存在未明漏洞、IBM PureApplication System 信息泄露漏洞。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-2015-03295>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03296>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03280>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03310>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03192>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03193>

4、Mozilla 产品安全漏洞

Mozilla Thunderbird 是由 Mozilla 浏览器的邮件功能部件所改造的邮件工具。Mozilla Firefox 是一款流行的开源 WEB 浏览器。本周，上述产品被披露存在信息泄露、内存错误引用和缓冲区溢出漏洞。攻击者可利用漏洞获取敏感信息或执行任意代码。

CNVD 收录的相关漏洞包括：Mozilla Thunderbird Linux Gstreamer 插件 H.264 视频处理缓冲区溢出漏洞、Mozilla Thunderbird SVG 内容和 CSS 处理缓冲区溢出漏洞、Mozilla Thunderbird 文本处理内存错误引用漏洞、Mozilla Thunderbird XML 内容解析缓冲区溢出漏洞、Mozilla Firefox on Android 信息泄露漏洞。其中“Mozilla Thunderbird XML 内容解析缓冲区溢出漏洞”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-2015-03181>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03182>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03127>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03183>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03184>

5、unzoo 'EntrReadArch'函数缓冲区溢出漏洞

unzoo 是一个文件解压缩包。本周，unzoo 被披露存在综合评级为“高危”的缓冲区溢出漏洞。攻击者利用该漏洞执行任意代码。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-2015-03245>

更多高危漏洞如表 3 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-2015-03178	SAP CRM Business Rules Framework SQL 注入漏洞	高	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞：

			https://service.sap.com/sap/support/
CNVD-2015-03179	SAP CRM Business Rules Framework 任意代码执行漏洞	高	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞： https://service.sap.com/sap/support/
CNVD-2015-03194	Linux kernel 'iov_iter_init'函数安全绕过漏洞	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.linux.com/
CNVD-2015-03196	GoAutoDial GoAdmin CE 'cpanel' action 变量任意命令执行漏洞	高	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞： http://goautodial.org/news/21
CNVD-2015-03210	PHP PHAR 'phar_tar_process_metadata()'函数堆内存破坏漏洞	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.php.net/downloads.php https://bugs.php.net/bug.php?id=69443&edit=2 http://git.php.net/?p=php-src.git;a=commit;h=17cbd0b5b78a7500f185b3781a2149881bfff8ae
CNVD-2015-03211	PHP 'str_repeat()'函数整数溢出漏洞	高	用户可联系供应商获得补丁信息： http://www.php.net/downloads.php
CNVD-2015-03224	Amazon App Store 远程代码执行漏洞	高	用户可联系供应商获得补丁信息： http://www.amazon.com/gp/mas/get/amazonapp
CNVD-2015-03221	TestDisk 'Check_OS2MB()'方法栈缓冲区溢出漏洞	高	用户可联系供应商获得补丁信息： http://www.cgsecurity.org/wiki/TestDisk
CNVD-2015-03220	GNS3 不可信搜索路径漏洞	高	用户可联系供应商获得补丁信息： http://www.gns3.com/
CNVD-2015-03218	InFocus IN3128HD 投影仪存在漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，Adobe 多款产品被披露存在多个安全漏洞，攻击者可利用漏洞执行任意代码。此外，Cisco、IBM、Mozilla 多款产品被披露存在多个安全漏洞，允许攻击者利用漏洞获取敏感信息、提升权限、进行跨站脚本和跨站请求伪造攻击、发起拒绝服务攻击或者执行任意代码。另外，unzoo 被披露存在一个高危零日漏洞，攻击者利用该漏洞可执行任意代码。建议相关用户应随时关注上述厂商主页，及时获取修复补丁或解决方案。

CNVD 整理和发布以下重要安全修补信息。

1、HP 修补 Access Control 产品漏洞

HP Access Control 允许用户通过启用了 NFC 功能的智能手机或平板电脑进行身份验证。

本周，HP 修补了上述产品存在的未授权访问漏洞，避免攻击者利用漏洞执行未授权操作。CNVD 已收录相关补丁，请广大用户及时下载更新，避免引发漏洞相关的网络安全事件。

补丁下载链接：<http://www.cnvd.org.cn/patchInfo/show/58781>

本周要闻速递

1. 路由器驱动组件 NetUSB 曝远程溢出漏洞

知名路由器 D-Link、NETGEAR、TP-LINK 上重要驱动组件 NetUSB 被曝存在严重的远程溢出漏洞，影响数以百万计的路由和嵌入式设备。这个漏洞是由奥地利安全公司 SEC Consult 的研究员 Stefan Viehbock 提交的，漏洞的编号为 CVE-2015-3036，当客户端发送计算机名到网络设备的服务端（TCP 端口 20005）时，同该端口建立连接后，就可以触发这个漏洞。黑客利用这个漏洞，可以轻松地在内核层面远程执行恶意代码，掌握路由等网络设备的生死命脉。

参考链接：<http://www.freebuf.com/news/67961.html>

2. 苹果 Safari 浏览器曝 URL 欺诈漏洞

苹果 Safari 浏览器曝出一个可被攻击者用作钓鱼攻击的新漏洞——当用户以为打开某个网站时，其实在访问另一个网址。例如，当用户在浏览 deusen.co.uk 网站内容时，浏览器地址栏中显示的却是 dailymail.co.uk 地址。

参考链接：<http://www.freebuf.com/news/67737.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