国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2015 年 04 月 06 日-2015 年 04 月 12 日 **2015 年第 15 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**低**。

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 112 个，其中高危漏洞 37 个、中危漏洞 68 个、低危漏洞 7 个。上述漏洞中，可利用来实施远程攻击的漏洞有 104 个。本周收录的漏洞中，已有 104 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“EMC Isilon OneFS 权限提升漏洞”、“Johnson Controls Metasys 无限制文件上传漏洞”等零日漏洞，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 112 个漏洞。报送情况如表 1 所示。其中，启明星辰、安天实验室、天融信、恒安嘉新等单位报送数量较多。此外， CNCERT 各分中心、乌云、漏洞盒子及白帽子向 CNVD 提交了 335 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
启明星辰	136	0
安天实验室	115	0
天融信	81	4
恒安嘉新	37	0
绿盟科技	31	0
知道创宇	1	0

乌云	256	256
漏洞盒子	49	49
CNCERT 宁夏分中心	10	10
CNCERT 福建分中心	2	2
CNCERT 安徽分中心	1	1
习科网络安全	1	1
个人	12	12
报送总计	732	335
录入总计	112（去重）	335

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Mozilla、Cisco、SAP 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	Mozilla	18	16%
2	Cisco	15	13%
3	SAP	10	9%
4	IBM	7	6%
5	Citrix	4	4%
6	ARJ Software, Inc.	3	3%
7	McAfee	3	3%
8	Wordpress	3	2%
9	Google	2	2%
10	其他	47	42%

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 112 个漏洞。其中应用程序漏洞 87 个，WEB 应用漏洞 9 个，网络设备漏洞 6 个，操作系统漏洞 5 个，安全产品漏洞 3 个，数据库漏洞 2 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	87
WEB 应用漏洞	9
网络设备漏洞	6
操作系统漏洞	5
安全产品漏洞	3
数据库漏洞	2

表 3 漏洞按影响类型统计表

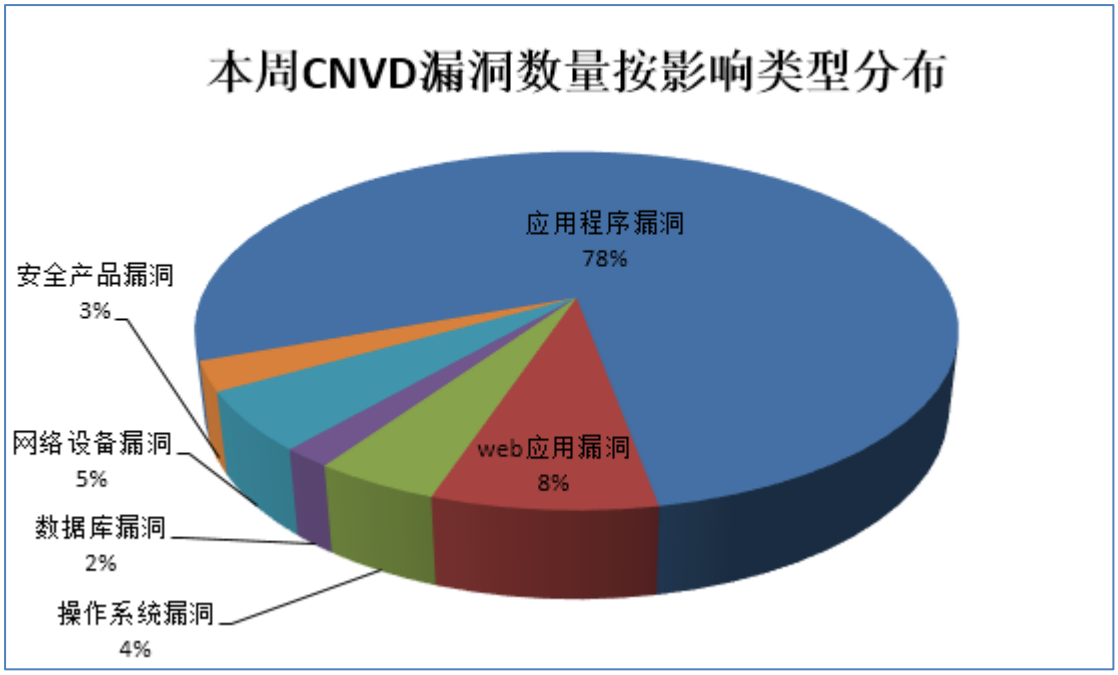

图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 9 个电信行业漏洞，2 个工控系统行业漏洞（如下图表所示）。其中，“SSL/TLS 协议加密算法 RC4 存在漏洞、IBM Tivoli Storage Manager FastBack 任意代码执行漏洞”的综合评级均为“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-2015-02171	SSL/TLS 协议加密算法 RC4 存在漏洞	高	是
电信	CNVD-2015-02172	10gen MongoDB 拒绝服务漏洞	中	是
电信	CNVD-2015-02239	Cisco Catalyst 4500 SNMP 轮询拒绝服务漏洞	中	是
电信	CNVD-2015-02238	Cisco ASR1000 系列路由器拒绝服务漏洞	中	是
电信	CNVD-2015-02237	Cisco Nexus 9000 Series 拒绝服务漏洞	中	是

电信	CNVD-2015-02272	Cisco Wireless LAN Controller HTML 帮助系统跨站脚本漏洞	中	否
电信	CNVD-2015-02270	IBM Tivoli Storage Manager FastBack 任意代码执行漏洞	高	是
电信	CNVD-2015-02293	IBM WebSphere DataPower XC10 appliance 会话劫持漏洞	中	是
电信	CNVD-2015-02290	Cisco ASR 拒绝服务漏洞	中	是
工控系统	CNVD-2015-02292	Siemens SIMATIC 和 SIMATIC WinCC HMI Comfort Panels 拒绝服务漏洞	中	是
工控系统	CNVD-2015-02291	Siemens SIMATIC 和 SIMATIC WinCC HMI Comfort Panels 验证绕过漏洞	中	是

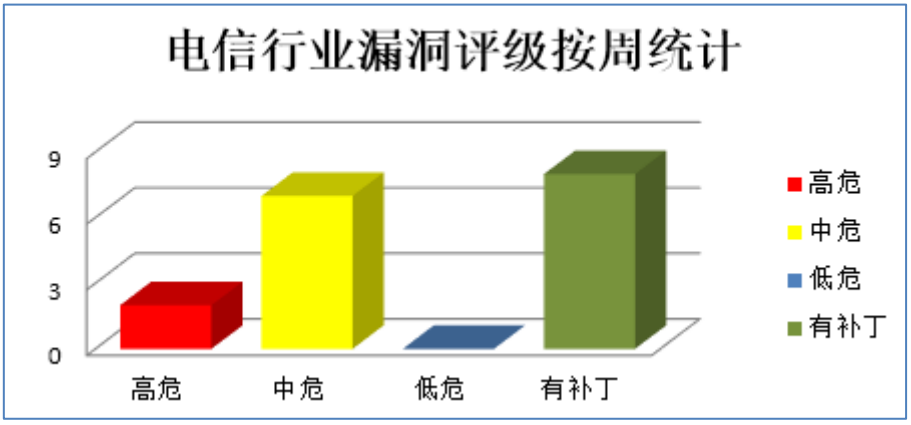

图 1 电信行业漏洞统计

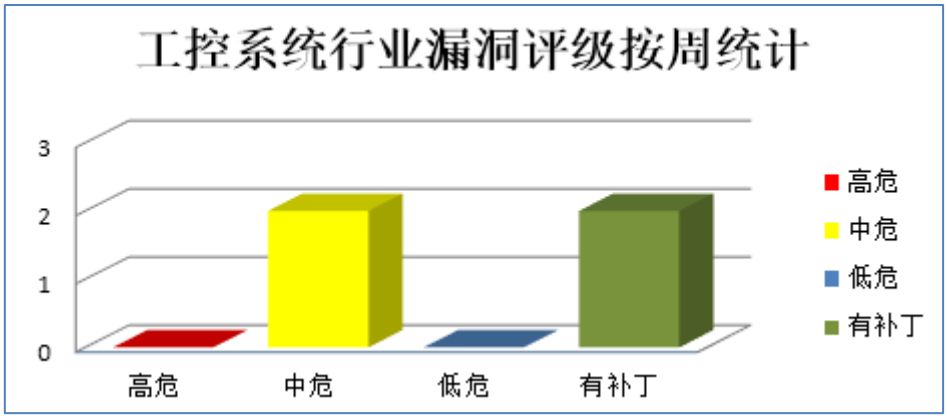

图 2 工控系统行业漏洞统计

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、 Mozilla 产品安全漏洞

Mozilla Firefox/SeaMonkey 是 Mozilla 所发布的 WEB 浏览器/新闻组客户端。本周，上述产品被披露存在权限提升、任意代码执行和拒绝服务漏洞，攻击者可利用漏洞提升权限、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：Mozilla Firefox/SeaMonkey 同源策略绕过权限提升漏洞、Mozilla Firefox 限制绕过权限访问漏洞、Mozilla Firefox 任意代码执行漏洞（CNVD-2015-02203、CNVD-2015-02207、CNVD-2015-02208）、Mozilla Firefox Off Main Thread Compositing (OMTC)实现任意代码执行漏洞、Mozilla Firefox 拒绝服务漏洞（CNVD-2015-02214）、Mozilla Firefox JavaScript 任意代码执行漏洞。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-2015-02261
http://www.cnvd.org.cn/flaw/show/CNVD-2015-02259
http://www.cnvd.org.cn/flaw/show/CNVD-2015-02203
http://www.cnvd.org.cn/flaw/show/CNVD-2015-02207
http://www.cnvd.org.cn/flaw/show/CNVD-2015-02208
http://www.cnvd.org.cn/flaw/show/CNVD-2015-02204
http://www.cnvd.org.cn/flaw/show/CNVD-2015-02214
http://www.cnvd.org.cn/flaw/show/CNVD-2015-02205

2、SAP 产品安全漏洞

SAP NetWeaver 是一款 SAP 业务套件解决方案、SAP xApps 组合应用、合作伙伴解决方案以及客户定制应用的技术基础。SAP Sybase SQL Anywhere 是一个数据库应用。SAP Mobile Platform 是一个企业移动平台。SAP Afaria 是一个移动设备管理解决方案。本周，上述产品被披露存在信息泄露、访问绕过、缓冲区溢出和拒绝服务漏洞，攻击者可利用漏洞获取敏感信息、绕过访问限制或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：SAP Afaria XcListener 访问绕过漏洞、SAP NetWeaver Portal XMLValidationComponent XXE 信息泄露漏洞、SAP NetWeaver Portal XXE 信息泄露漏洞、SAP NetWeaver SAP 管理控制台敏感信息获取漏洞、SAP Sybase SQL Anywhere 存在未明拒绝服务漏洞、SAP Mobile Platform XXE 信息泄露漏洞（CNVD-2015-02245）、SAP Mobile Platform XXE 信息泄露漏洞、SAP Afaria XcListener 缓冲区溢出漏洞。其中，“SAP Afaria XcListener 访问绕过漏洞”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-2015-02250
http://www.cnvd.org.cn/flaw/show/CNVD-2015-02244
http://www.cnvd.org.cn/flaw/show/CNVD-2015-02243

http://www.cnvd.org.cn/flaw/show/CNVD-2015-02242

http://www.cnvd.org.cn/flaw/show/CNVD-2015-02260

http://www.cnvd.org.cn/flaw/show/CNVD-2015-02245

http://www.cnvd.org.cn/flaw/show/CNVD-2015-02246

http://www.cnvd.org.cn/flaw/show/CNVD-2015-02249

3、Cisco 产品安全漏洞

Cisco Prime Data Center Network Manager 是一个网络管理应用，可帮助您有效执行和管理虚拟化数据中心。Cisco Unity Connection 是一个功能丰富的语音留言平台，采用 Linux 统一通信操作系统。Cisco Unified Communications Manager 是企业级 IP 电话呼叫处理系统。本周，上述产品被披露存在信息泄露和拒绝服务漏洞。攻击者可利用漏洞获取敏感信息或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco Prime Data Center Network Manager 文件信息泄露漏洞（CNVD-2015-02229）、Cisco Unity Connection SIP 中继集成端口 UDP 5060 拒绝服务漏洞、Cisco Unity Connection SIP 中继集成端口拒绝服务漏洞、Cisco Unity Connection SIP 中继集成 CuCsMgr 拒绝服务漏洞、Cisco Unity Connection SIP 中继集成特制 INVITE 消息拒绝服务漏洞（CNVD-2015-02212、CNVD-2015-02193）、Cisco Prime Data Center Network Manager 文件信息泄露漏洞、Cisco CUCDM 信息泄露漏洞。其中，除“Cisco CUCDM 信息泄露漏洞”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-2015-02229

http://www.cnvd.org.cn/flaw/show/CNVD-2015-02211

http://www.cnvd.org.cn/flaw/show/CNVD-2015-02210

http://www.cnvd.org.cn/flaw/show/CNVD-2015-02209

http://www.cnvd.org.cn/flaw/show/CNVD-2015-02212

http://www.cnvd.org.cn/flaw/show/CNVD-2015-02193

http://www.cnvd.org.cn/flaw/show/CNVD-2015-02194

http://www.cnvd.org.cn/flaw/show/CNVD-2015-02192

4、Citrix 产品安全漏洞

Citrix NetScaler 是一款网络流量管理产品。本周，上述产品被披露存在跨站脚本、跨站请求伪造和访问限制绕过漏洞。攻击者可利用漏洞绕过访问限制、进行跨站脚本攻击或执行任意命令。

CNVD 收录的相关漏洞包括：Citrix NetScaler Nitro API 跨站请求伪造漏洞、Citrix NetScaler Nitro help/rt/large_search.html 跨站脚本漏洞、Citrix NetScaler Citrix NetScaler AppFirewall 访问限制绕过漏洞、Citrix NetScaler Nitro API 跨站脚本漏洞。目前，

除“Citrix NetScaler Citrix NetScaler AppFirewall 访问限制绕过漏洞“外，厂商已经发布了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-2015-02233

http://www.cnvd.org.cn/flaw/show/CNVD-2015-02232

http://www.cnvd.org.cn/flaw/show/CNVD-2015-02231

http://www.cnvd.org.cn/flaw/show/CNVD-2015-02230

5、WordPress 插件 Simple Ads Manager SQL 注入漏洞

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。Simple Ads Manager 是其中的一个用于管理广告的插件。本周，WordPress 插件 Simple Ads Manager 被披露存在综合评级为“高危”的 SQL 注入漏洞。攻击者利用该漏洞执行任意 SQL 命令。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-2015-02178

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-2015-02180	HP Integrated Lights-Out 存在未明代码执行漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://h20564.www2.hp.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c04486432
CNVD-2015-02181	IBM Domino LDAP Server 任意代码执行漏洞	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：http://www-01.ibm.com/support/docview.wss?uid=swg21700029
CNVD-2015-02199	EMC Isilon OneFS 权限提升漏洞	高	暂无
CNVD-2015-02198	Johnson Controls Metasys 无限制文件上传漏洞	高	暂无
CNVD-2015-02271	IBM Rational ClearCase GSKit 加密问题漏洞	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-01.ibm.com/support/docview.wss?uid=swg21698893
CNVD-2015-02270	IBM Tivoli Storage Manager FastBack 任意代码执行漏洞	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：

			http://www-01.ibm.com/support/docview.wss?uid=swg21699645
CNVD-2015-02269	IBM Domino SSLv2 缓冲区溢出漏洞	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-01.ibm.com/support/docview.wss?uid=swg21700029
CNVD-2015-02285	Oxide 内存错误引用漏洞	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://bugs.launchpad.net/oxide/+bug/1431484
CNVD-2015-02283	Open-source ARJ archiver 缓冲区溢出漏洞	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://www.debian.org/security/2015/dsa-3213
CNVD-2015-02289	Apache Subversion mod_dav_svn 拒绝服务漏洞	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://subversion.apache.org/security/CVE-2015-0202-advisory.txt

表 3 部分高危漏洞列表

小结：本周，Mozilla 被披露存在权限提升、任意代码执行和拒绝服务漏洞，攻击者可利用漏洞提升权限、执行任意代码或发起拒绝服务攻击。此外，SAP、Cisco、Citrix 多款产品被批露存在多个安全漏洞，允许攻击者利用漏洞获取敏感信息、进行跨站攻击、绕过访问限制、执行任意代码或发起拒绝服务攻击。另外，WordPress 插件 Simple Ads Manager 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 SQL 命令。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。

本周重要漏洞修补信息

CNVD 整理和发布以下重要安全修补信息。

1、Linux 修补 Kernel 产品漏洞

Linux kernel 是一款开源的操作系统。

本周，Linux 修补了上述产品存在的信息泄露和拒绝服务漏洞，避免攻击者利用漏洞获取敏感信息或发起拒绝服务攻击。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/57150

http://www.cnvd.org.cn/patchInfo/show/57020

本周要闻速递

1. 流行 WordPress 缓存插件 WP-Super-Cache 曝高危安全漏洞

流行 WordPress 缓存插件 WP-Super-Cache 近日曝出高危漏洞，攻击者可以使用一个精心构造的查询语句向插件缓存文件列表页面中插入恶意脚本。注入的恶意脚本会执行一系列恶劣且猥琐的事情，比如添加一个管理员账户、注入后门等。

参考链接：http://www.freebuf.com/news/63393.html

2. 戴尔支持软件（Dell System Detect）存在安全漏洞，可被远程执行恶意代码

预装在戴尔电脑上的支持软件 Dell System Detect 被发现存在漏洞， 允许攻击者远程执行恶意代码。System Detect 是戴尔系统捆绑式的一个软件，只要系统启动，它就会随之自动启动。通常攻击者会引诱用户访问恶意网站，并且恶意网站只要域名中含有 dell 字符串就能利用这个漏洞感染系统。如果受害者设备感染了这一漏洞，那设备上的一些凭证，诸如各种账号，密码，姓名，地址等就有可能被攻击者窃取，更为甚的是，攻击者还可能会损毁受害者的设备。

参考链接：http://www.freebuf.com/news/63259.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