国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2015 年 10 月 19 日-2015 年 10 月 25 日　　2015 年第 43 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 177 个，其中高危漏洞 104 个、中危漏洞 61 个、低危漏洞 12 个。上述漏洞中，可利用来实施远程攻击的漏洞有 161 个。本周收录的漏洞中，已有 172 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“Konica Minolta FTP Utility 拒绝服务漏洞”、“Konica Minolta FTP Utility 缓冲区溢出漏洞”等零日代码攻击，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 177 个漏洞。报送情况如表 1 所示。其中，奇虎(补天平台)、天融信、启明星辰、安天实验室等单位报送数量较多。此外，乌云、漏洞盒子、习科网络安全、腾讯玄武实验室及白帽子向 CNVD 提交了 751 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)	341	341
天融信	218	0
启明星辰	136	0
安天实验室	130	0
恒安嘉新	21	0
乌云	336	336

漏洞盒子	21	21
习科网络安全	1	1
腾讯玄武实验室	1	1
CNCERT 福建分中心	2	2
个人	49	49
报送总计	1256	751
录入总计	177（去重）	751

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、Microsoft、Google 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	73	41%
2	Microsoft	29	16%
3	Google	10	6%
4	Apple	8	5%
5	SAP	7	4%
6	CloudBees	6	3%
7	revive-adserver	6	3%
8	EMC	4	2%
9	SolarWinds	3	2%
10	其他	31	18%

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 177 个漏洞。其中应用程序漏洞 146 个，操作系统漏洞 17 个，Web 应用漏洞 6 个，数据库漏洞 6 个，网络设备漏洞 2 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	146
操作系统漏洞	17
Web 应用漏洞	6

数据库漏洞	6
网络设备漏洞	2

表 3 漏洞按影响类型统计表

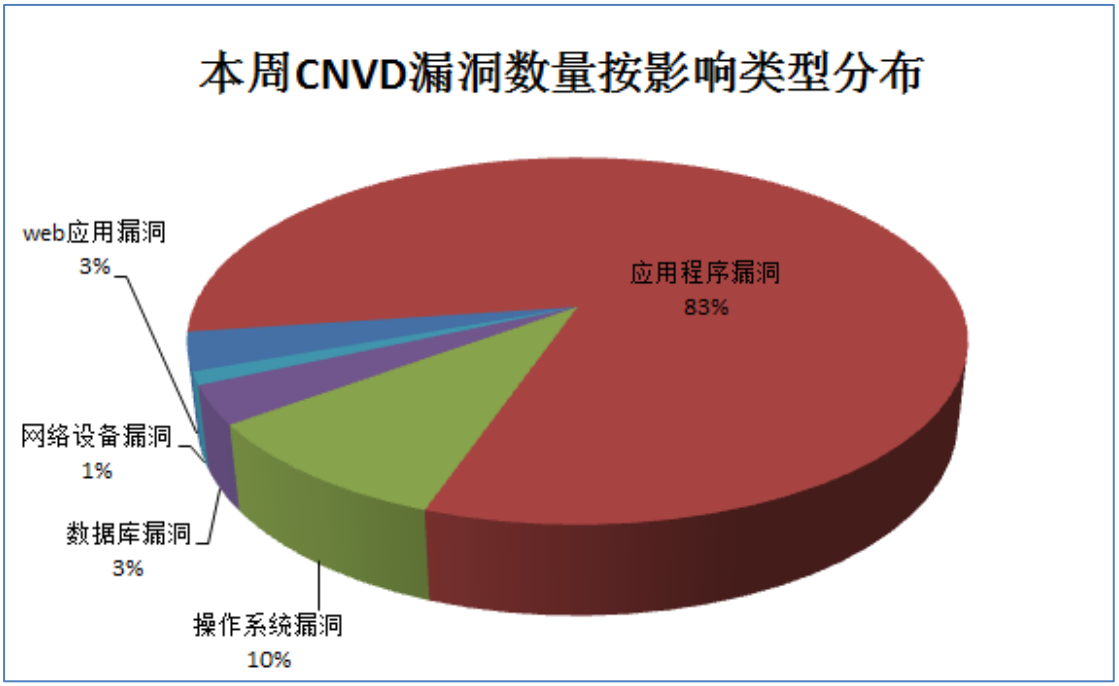

图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 2 个电信行业漏洞、2 个工系统行业漏洞（如下图表所示）。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-2015-06771	IBM AIX 和 VIOS netstat 权限提升漏洞	中	是
电信	CNVD-2015-06780	Cisco Wireless LAN Controller 客户端断开连接漏洞	中	是
工控系统	CNVD-2015-06785	3S CODESYS Runtime Toolkit 空指针间接引用漏洞	中	是
工控系统	CNVD-2015-06784	Nordex NC2 存在多个跨站脚本漏洞	中	是

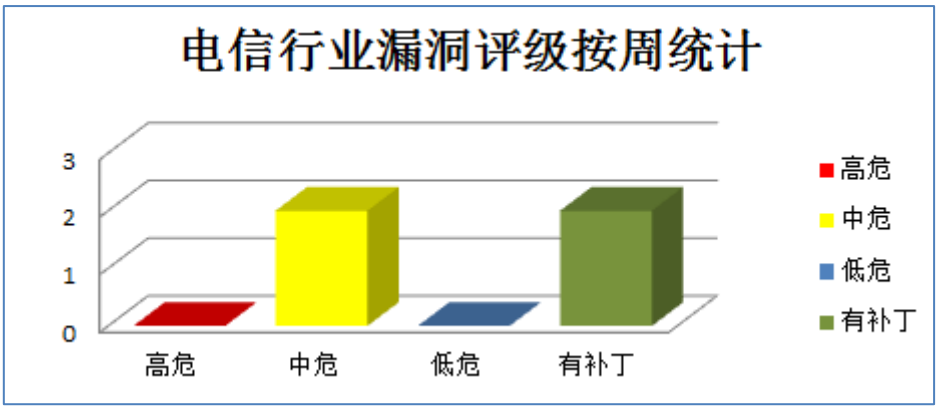

图 1 电信行业漏洞统计

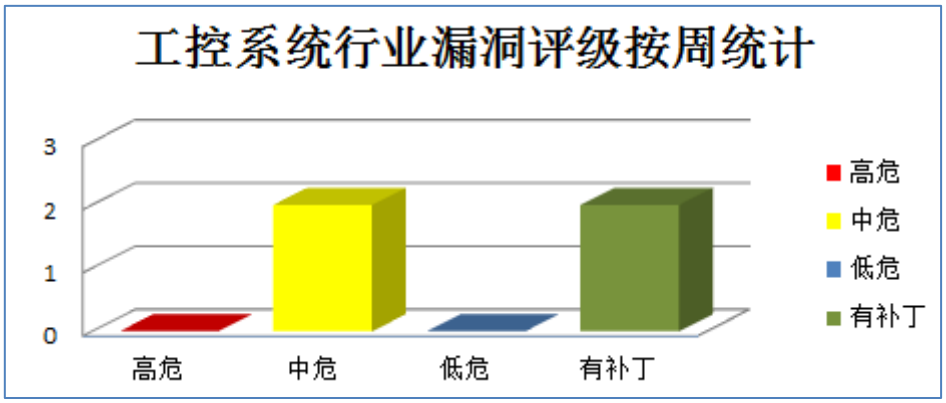

图 2 工控系统行业漏洞统计

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、Microsoft 产品安全漏洞

Internet Explorer 是微软公司推出的一款网页浏览器。本周，该产品被披露存在内存破坏、权限提升和信息泄露漏洞。攻击者利用漏洞可执行任意代码、提升权限和获得敏感信息。

CNVD 收录的相关漏洞包括：Microsoft Internet Explorer 内存破坏漏洞（CNVD-2015-06652、CNVD-2015-06654、CNVD-2015-06656）、Microsoft Internet Explorer 权限提升漏洞（CNVD-2015-06626、CNVD-2015-06655、CNVD-2015-06657）、Microsoft Internet Explorer 信息泄露漏洞（CNVD-2015-06653、CNVD-2015-06658）。其中，“Microsoft Internet Explorer 内存破坏漏洞（CNVD-2015-06652、CNVD-2015-06654、CNVD-2015-06656）”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-2015-06652

http://www.cnvd.org.cn/flaw/show/CNVD-2015-06654

http://www.cnvd.org.cn/flaw/show/CNVD-2015-06656
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06626
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06655
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06657
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06653
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06658

2、 Google 产品安全漏洞

Google Chrome 是一款开源的 WEB 浏览器。本周，该产品被披露存在多个安全漏洞。攻击者利用漏洞可获取敏感信息、执行任意代码和发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Google Chrome 存在未明漏洞（CNVD-2015-06765）、Google Chrome V8 拒绝服务漏洞（CNVD-2015-06766）、Google Chrome libANGLE 代码注入漏洞、Google Chrome Blink 同源策略绕过漏洞（CNVD-2015-06764、CNVD-2015-06769）、Google Chrome ServiceWorker 内存错误引用漏洞、Google Chrome Blink ‘shouldTreatAsUniqueOrigin’函数信息泄露漏洞、Google Chrome FFmpeg 竞争条件漏洞。其中，除“Google Chrome Blink ‘shouldTreatAsUniqueOrigin’函数信息泄露漏洞、Google Chrome FFmpeg 竞争条件漏洞”外，其余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-2015-06765
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06766
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06762
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06764
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06769
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06767
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06761
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06763

3、 Adobe 产品安全漏洞

Adobe Flash Player 是一款 Flash 文件处理程序。本周，该产品被披露存在内存错误引用和内存破坏漏洞。攻击者利用漏洞可执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Flash Player 内存错误引用漏洞（CNVD-2015-06676、CNVD-2015-06677、CNVD-2015-06680、CNVD-2015-06681、CNVD-2015-06682）、Adobe Flash Player 内存破坏漏洞（CNVD-2015-06668、CNVD-2015-06669、CNVD-2015-06670）。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-2015-06676

http://www.cnvd.org.cn/flaw/show/CNVD-2015-06677

http://www.cnvd.org.cn/flaw/show/CNVD-2015-06680

http://www.cnvd.org.cn/flaw/show/CNVD-2015-06681

http://www.cnvd.org.cn/flaw/show/CNVD-2015-06682

http://www.cnvd.org.cn/flaw/show/CNVD-2015-06668

http://www.cnvd.org.cn/flaw/show/CNVD-2015-06669

http://www.cnvd.org.cn/flaw/show/CNVD-2015-06670

4、SAP 产品安全漏洞

SAP HANA DB 是一个基于行和列的内存数据库。本周，上述产品被披露存在跨站脚本、SQL 注入和拒绝服务漏洞。攻击者利用漏洞可进行跨站脚本攻击、获得敏感信息和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：SAP HANA DB 跨站脚本漏洞（CNVD-2015-06777、CNVD-2015-06778）、SAP HANA DB SQL 注入漏洞（CNVD-2015-06775、CNVD-2015-06776）、SAP HANA Developer Edition DB Eval 注入漏洞、SAP HANA hdbsql 客户端拒绝服务漏洞。其中，“SAP HANA hdbsql 客户端拒绝服务漏洞”的综合评级为“高危”。目前，厂商已发布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-2015-06777

http://www.cnvd.org.cn/flaw/show/CNVD-2015-06778

http://www.cnvd.org.cn/flaw/show/CNVD-2015-06775

http://www.cnvd.org.cn/flaw/show/CNVD-2015-06776

http://www.cnvd.org.cn/flaw/show/CNVD-2015-06700

http://www.cnvd.org.cn/flaw/show/CNVD-2015-06774

5、MoxaOnCell Central Manager Server RequestController 远程代码执行漏洞

MoxaOnCell Central Manager 可以通过 Web 访问私有 IP 网络设备。本周，MoxaOnCell Central Manager 被披露存在综合评级为“高危”的远程代码执行漏洞。攻击者利用该漏洞可执行任意代码。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-2015-06671

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-2015-06627	ZOHO ManageEngineOpManager 硬编码凭证漏洞	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://support.zoho.com/portal/manageengine/helpcenter/articles/pgsql-submitquery-do-vulnerability
CNVD-2015-06632	EMC SourceOne Email Supervisor 会话劫持漏洞	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：http://www.emc.com/data-protection/emc-sourceone/email-supervisor.htm
CNVD-2015-06650	CybozuGaroon 代码注入漏洞	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://support.cybozu.com/ja-jp/article/8811
CNVD-2015-06649	CybozuGaroon RSS Reader 组件代码注入漏洞	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://support.cybozu.com/ja-jp/article/8810
CNVD-2015-06702	SolarWinds Log and Event Manager 任意代码执行漏洞（CNVD-2015-06702）	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.solarwinds.com/documentation/lem/docs/releasenotes/releasenotes.htm
CNVD-2015-06703	SolarWinds Log and Event Manager 任意代码执行漏洞（CNVD-2015-06703）	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.solarwinds.com/documentation/lem/docs/releasenotes/releasenotes.htm
CNVD-2015-06710	Revive Adserver 未授权操作漏洞	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：http://www.revive-adserver.com/security/revive-sa-2015-001/
CNVD-2015-06708	Revive Adserver Flash cross-domain 跨域攻漏洞	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：http://www.revive-adserver.com/security/revive-sa-2015-001/
CNVD-2015-06770	SolarWinds Storage Manager 文件上传并执行漏洞	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://www.solarwinds.com/documentation/lem/docs/releasenotes/releasenotes.htm

CNVD-2015-06773	QNAP Systems QNAP QTS 目录遍历漏洞	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://www.qnap.com/i/en/support/con_show.php?cid=85

表 3 部分高危漏洞列表

小结：本周，Microsoft 产品被披露存在内存破坏、权限提升和信息泄露漏洞。攻击者利用漏洞可执行任意代码、提升权限和获得敏感信息。此外，Google、Adobe、SAP 多款产品被披露存在多个安全漏洞，攻击者利用漏洞可获得敏感信息、进行跨站脚本攻击、执行任意代码和发起拒绝服务攻击。另外，MoxaOnCell Central 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。

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 是美国 Linux 基金会发布的操作系统 Linux 所使用的内核。

本周，Linux 修补了上述产品存在的竞争条件和拒绝服务漏洞，避免攻击者利用漏洞获取权限和发起拒绝服务攻击。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/65595

http://www.cnvd.org.cn/patchInfo/show/65516

本周要闻速递

1. Magento 网站被攻击并传播恶意软件

Sucuri 的安全专家们发现异常针对 Magento 电商平台的大量恶意软件攻击。这场攻击行动也同时被 Malwarebytes 的研究人员们发现了，他们的研究方向主要是在客户端侧。攻击者攻陷了运行 Magento 的网站，并注入了恶意代码，在网站上显示来自“guruincsite.com”域名的 iframe。他们通过利用一个目录遍历漏洞攻击 Magento 网站，这个漏洞存在于第三方的大量导入工具 Magmi。安全公司们都知道 guruincsite 域名，根据 Google Safe Browsing 的数据，这个域名已经被用来感染 8000 多个域名。

参考链接：http://www.freebuf.com/news/82422.html

2. 英国电信运营商 TalkTalk 数据泄露，影响 4 百万用户

TalkTalk 是英国一家手机通信及宽带服务的运营商，但目前因为其网站被攻击，可能导致 TalkTalk 用户个人信息以及银行账号等数据遭受泄露。TalkTalk 目前确认，此次网络攻击是有针对性的黑客行为，危及了包含用户的个人和银行账户等信息。据称，因

TalkTalk 系统中部分用户数据并没有采取加密，所以存在泄露的风险（具体是哪些数据，目前 TalkTalk 并未公布）。据悉，目前为保护数据的安全，TalkTalk 已经将其网站下线，并对其中的数据进行检查。

参考链接：http://www.freebuf.com/news/82832.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