国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2015 年 08 月 31 日-2015 年 09 月 06 日 **2015 年第 36 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 92 个，其中高危漏洞 40 个、中危漏洞 43 个、低危漏洞 9 个。上述漏洞中，可利用来实施远程攻击的漏洞有 83 个。本周收录的漏洞中，已有 84 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“GSM SIM Utility 栈缓冲区溢出漏洞”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 92 个漏洞。报送情况如表 1 所示。其中，奇虎、绿盟科技、天融信、启明星辰等单位报送数量较多。此外，CNCERT 各分中心、乌云、漏洞盒子、High-Tech Bridge Security Research 及白帽子向 CNVD 提交了 547 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	228	228
绿盟科技	165	0
天融信	116	0
启明星辰	58	0
安天实验室	57	0
恒安嘉新	1	0

乌云	261	261
漏洞盒子	48	48
CNCERT 甘肃分中心	4	4
High-Tech Bridge Security Research	1	1
个人	5	5
报送总计	944	547
录入总计	92（去重）	547

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 HP、Cisco、Wireshark 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	HP	28	32%
2	Cisco	11	12%
3	Wireshark	10	11%
4	IBM	5	5%
5	OpenSSH	3	3%
6	SAP	3	3%
7	Apple	2	2%
8	Drupal	2	2%
9	Mozilla	2	2%
10	其他	26	28%

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 92 个漏洞。其中应用程序漏洞 77 个，网络设备漏洞 9 个，操作系统漏洞 3 个，Web 应用漏洞 3 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	77
网络设备漏洞	9

操作系统漏洞	3
Web 应用漏洞	3

表 3 漏洞按影响类型统计表

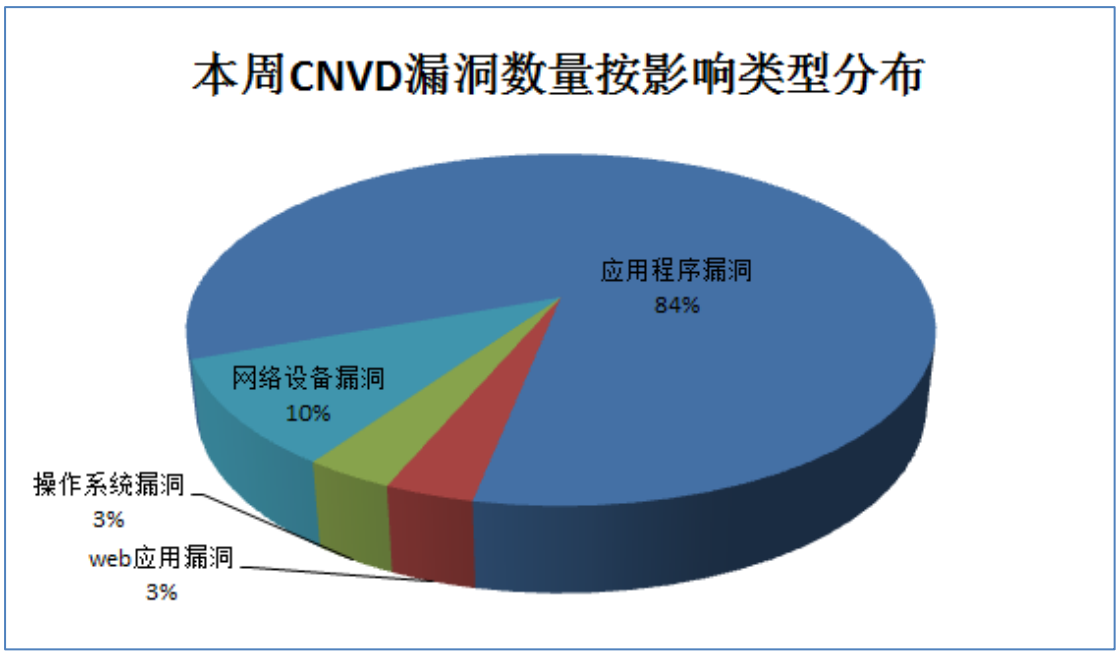

图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 12 个电信行业漏洞、1 个移动互联网行业漏洞、2 个工控系统行业漏洞（如下图表所示）。其中，“Cisco ASR 1000 Series Router UDP 报文处理拒绝服务漏洞、Cisco ASR 1000 Series Router IOS XE VFR 拒绝服务漏洞、Cisco ASR 1000 Series Router L2TP 处理拒绝服务漏洞、Cisco ASR 1000 Series Router IP 报文处理拒绝服务漏洞、Cisco ASR 1000 Series Router IPv6 报文处理拒绝服务漏洞、Cisco ASR 1000 Series Router SIP 报文处理拒绝服务漏洞、Cisco ASR 1000 Series Router H.323 报文处理拒绝服务漏洞”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-2015-05727	Wireshark GSM RLC/MAC 解析器拒绝服务漏洞	中	是
电信	CNVD-2015-05747	Cisco ASR 1000 Series Router UDP 报文处理拒绝服务漏洞	高	是
电信	CNVD-2015-05748	Cisco ASR 1000 Series Router IOS XE VFR 拒绝服务漏洞	高	是
电信	CNVD-2015-05749	Cisco ASR 1000 Series Router L2TP 处理拒绝服务漏洞	高	是

电信	CNVD-2015-05750	Cisco ASR 1000 Series Router IP 报文处理拒绝服务漏洞	高	是
电信	CNVD-2015-05746	Cisco ASR 1000 Series Router IPv6 报文处理拒绝服务漏洞	高	是
电信	CNVD-2015-05745	Cisco ASR 1000 Series Router SIP 报文处理拒绝服务漏洞	高	是
电信	CNVD-2015-05744	Cisco ASR 1000 Series Router H.323 报文处理拒绝服务漏洞	高	是
电信	CNVD-2015-05765	IBM WebSphere Application Server 敏感信息泄露漏洞	低	是
电信	CNVD-2015-05766	IBM WebSphere Application Server 和 WebSphere Virtual Enterprise 信息泄露漏洞	中	是
电信	CNVD-2015-05781	Cisco Application Control Engine 4700 A5 安全绕过漏洞	中	是
电信	CNVD-2015-05793	GSM SIM Utility 栈缓冲区溢出漏洞	高	否
移动互联网	CNVD-2015-05784	SAP Afaria Device Inspector 页面跨站脚本漏洞	中	否
工控系统	CNVD-2015-05740	Schneider Electric Modicon M340 PLC Station P34 Module Modicon 存在多个漏洞	高	否
工控系统	CNVD-2015-05789	Siemens SIMATIC S7-1200 CPU 设备跨站请求伪造漏洞	中	是

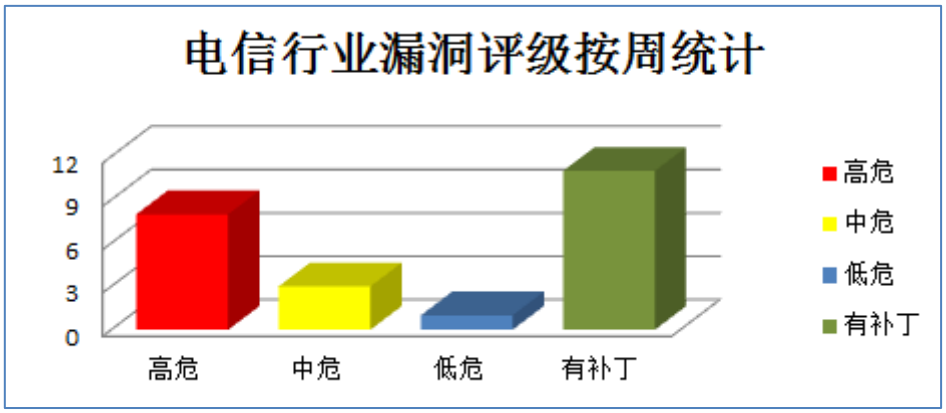

图 1 电信行业漏洞统计

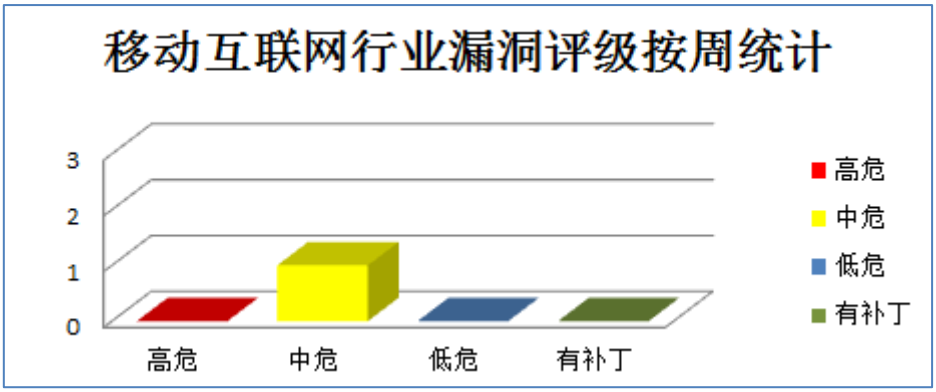

图 2 移动互联网行业漏洞统计

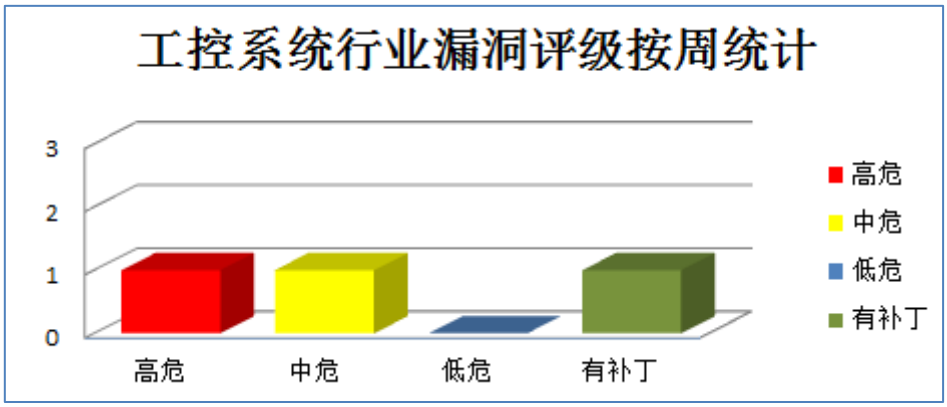

图 3 工控系统行业漏洞统计

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、Cisco 产品安全漏洞

Cisco ASR1000 系列汇聚服务路由器，提供了广域网边缘解决方案，将信息、通信、协作和商务融为一体。Cisco Identity Services Engine 身份服务引擎一款用于 Cisco TrustSec 解决方案的中央策略引擎。本周，上述产品被披露存在访问控制绕过和拒绝服务漏洞。攻击者利用漏洞可绕过访问控制权限和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco ASR 1000 Series Router L2TP 处理拒绝服务漏洞、Cisco ASR 1000 Series Router IP 报文处理拒绝服务漏洞、Cisco ASR 1000 Series Router IPv6 报文处理拒绝服务漏洞、Cisco ASR 1000 Series Router SIP 报文处理拒绝服务漏洞、Cisco ASR 1000 Series Router H.323 报文处理拒绝服务漏洞、Cisco ASR 1000 Series Router UDP 报文处理拒绝服务漏洞、Cisco ASR 1000 Series Router IOS XE VFR 拒绝服务漏洞、Cisco Identity Services Engine 访问控制绕过漏洞。其中，除“Cisco Identity Services Engine 访问控制绕过漏洞”外，其余漏洞的综合评级为“高危”。目前，厂商已经发布了除“Cisco Identity Services Engine 访问控制绕过漏洞”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-2015-05749

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05750

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05746

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05745

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05744

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05747

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05748

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05751

2、 HP 产品安全漏洞

HP KeyView 是文件过滤及转换软件，可提取文件内容和元数据。本周，上述产品被披露存在远程代码执行漏洞。攻击者利用漏洞可执行任意代码。

CNVD 收录的相关漏洞包括：HP KeyView 任意代码执行漏洞（CNVD-2015-05714、CNVD-2015-05715、CNVD-2015-05716、CNVD-2015-05717、CNVD-2015-05718、CNVD-2015-05719、CNVD-2015-05720、CNVD-2015-05730）。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-2015-05714

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05715

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05716

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05717

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05718

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05719

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05720

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05730

3、 OpenSSH 产品安全漏洞

OpenSSH（OpenBSD Secure Shell）on non-OpenBSD platforms 是 OpenBSD 计划组所维护的一套运行于非 OpenBSD（基于 BSD 的 UNIX 实现）平台且用于安全访问远程计算机的连接工具。本周，上述产品被披露存在输入验证、内存错误引用和拒绝服务漏洞。攻击者可利用漏洞进行伪造攻击、获取权限和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：OpenSSH sshd monitor 组件输入验证漏洞、OpenSSH sshd monitor.c 文件内存错误引用漏洞、OpenSSH sshd 拒绝服务漏洞。其中，“OpenSSH sshd 拒绝服务漏洞”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-2015-05761

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05760

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05759

4、SAP 产品安全漏洞

SAP NetWeaver 是德国思爱普（SAP）公司的一套面向服务的集成化应用平台，它可为 SAP 应用提供开发和运行环境。SAP NetWeaver Portal 是其中的一套门户网站解决方案，它通过 Web 浏览器提供单点登录信息进行身份验证。SAP Afaria 是德国思爱普（SAP）公司的一套移动设备管理解决方案。该方案支持对移动设备、应用及数据生命周期进行有效管理，并确保其在传输和存储过程中的安全性。SAP Mobile Platform（SMP）是德国思爱普（SAP）公司的一套移动应用开发平台。该平台用于构建适用于任意 XML 外部实体和跨站脚本漏洞。攻击者可利用漏洞读取任意文件和进行跨站脚本攻击。

CNVD 收录的相关漏洞包括：SAP NetWeaver Portal XML 外部实体漏洞、SAP Afaria Device Inspector 页面跨站脚本漏洞、SAP Mobile Platform application import XML 外部实体漏洞。目前，厂商尚未发布上述漏洞的修补程序。

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2015-05783

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05784

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05785

5、Schneider Electric Modicon M340 PLC Station P34 Module Modicon 存在多个漏洞

Schneider Electric Modicon M340 PLC 是用于工业进程和架构的中型 PLC 平台。本周，Modicon M340 PLC Station P34 模块被披露存在多个综合评级为“高危”的安全漏洞。攻击者利用该漏洞可获得敏感信息、绕过身份验证和执行任意代码。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-2015-05740

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-2015-05711	HP Matrix Operating Environment 信息泄露漏洞（CNVD-2015-05711）	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/hpsc/doc/public/display?docId=emr_na-c04774019
CNVD-2015-05710	HP Matrix Operating Environment 信息泄露漏洞（CNVD-2015-05710）	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/hpsc/doc/public/display?docId=emr_na-c04774019

CNVD-2015-05709	HP Matrix Operating Environment 信息泄露漏洞（CNVD-2015-05709）	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/hpsc/doc/public/display?docId=emr_na-c04774019
CNVD-2015-05707	HP Matrix Operating Environment Systems Insight Manager 信息泄露漏洞（CNVD-2015-05707）	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/hpsc/doc/public/display?docId=emr_na-c04774019
CNVD-2015-05705	HP Matrix Operating Environment Systems Insight Manager 信息泄露漏洞（CNVD-2015-05705）	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/hpsc/doc/public/display?docId=emr_na-c04774019
CNVD-2015-05733	PolarSSL 内存泄露漏洞	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://lists.opensuse.org/opensuse-updates/2014-11/msg00079.html
CNVD-2015-05734	HP Version Control Repository Manager 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：https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c04765115
CNVD-2015-05741	多个 Foxit 产品远程代码执行漏洞	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：http://www.foxitsoftware.com/products/mobilereader/
CNVD-2015-05755	多款 F5 产品拒绝服务漏洞	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：https://support.f5.com/kb/en-us/solutions/public/17000/000/sol17047.html
CNVD-2015-05758	多款 Adobe 产品内存错误引用漏洞（CNVD-2015-05758）	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://helpx.adobe.com/security/products/flash-player/apsb15-19.html

表 3 部分高危漏洞列表

小结：Cisco 产品被披露存在访问控制绕过和拒绝服务漏洞。攻击者利用漏洞可绕过访问控制权限和发起拒绝服务攻击。此外，HP、OpenSSH、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、执行任意代码或发起拒绝服务攻击。另外，Modicon M340 PLC Station P34 模块被披露存在一个高

危零日漏洞，攻击者利用该漏洞可获得敏感信息、绕过身份验证和执行任意代码。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 Linux 操作系统的内核。

本周，Linux 修补了上述产品存在的拒绝服务漏洞，避免攻击者利用漏洞发起拒绝服务攻击。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/63342

本周要闻速递

1. Corebot：一个高度模块化的信息窃取软件

IBM 发现了一种新型的数据窃取恶意软件，叫做 Corebot。它是一个高度模块化的恶意软件，一些安全检测系统会将 CoreBot 识别为 Dynamer!ac 或者 Eldorado。它专门窃取系统、邮件凭证，还有软件密钥，甚至还可以下载并执行其他的一些恶意程序。

参考链接：http://www.freebuf.com/news/76930.html

2. UPnP 曝 Filet-O-Firewall 漏洞，数百万家庭路由器处于攻击风险之中

导致 UPnP 中漏洞的主要原因在于，其缺乏足够的身份验证机制。如果成功利用了 Filet-o-Firewall 漏洞，那么攻击者将能够打开防火墙端口，并向家用路由器发送管理命令。有研究员解释说，在不到 20 秒内就能发起这种攻击，并且任何运行了 UPnP 服务的家庭路由器都处于这种攻击风险之中。具有关报告显示，作为一种缓解措施，建议用户禁用 UPnP 来随机化 UPnP UUID 和 URL。

参考链接：http://www.freebuf.com/news/77057.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