

信息安全漏洞周报

2015 年 07 月 20 日-2015 年 07 月 26 日

2015 年第 30 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 191 个，其中高危漏洞 77 个、中危漏洞 89 个、低危漏洞 25 个。上述漏洞中，可利用来实施远程攻击的漏洞有 142 个。本周收录的漏洞中，已有 182 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“TOTOLINK Router Models 代码执行漏洞”、“D-Link Cookie 命令注入漏洞”等零日攻击代码，请使用相关产品的用户注意加强防范。

本周，OpenSSH 最新版本曝高危 Oady 漏洞，攻击者可越过登录次数限制，不断尝试登录 OpenSSH 服务器，导致 Linux 主机面临暴力破解威胁，请广大用户关注厂商发布的漏洞修复情况及时修补。

成员单位报送漏洞统计

本周，共 8 家成员单位、合作伙伴及个人报送了本周收录的全部 191 个漏洞。报送情况如表 1 所示。其中，安天实验室、启明星辰、天融信、奇虎等单位报送数量较多。此外，CNCERT 各分中心、四川大学信息安全研究所、乌云、漏洞盒子、High-Tech Bridge Security Research Lab 及白帽子向 CNVD 提交了 669 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
安天实验室	237	0
启明星辰	234	0
天融信	227	13
奇虎	203	203

绿盟科技	192	0
恒安嘉新	26	0
东软	8	0
知道创宇	5	0
High-Tech Bridge Security Research Lab	2	2
乌云	369	369
漏洞盒子	58	58
四川大学信息安全研 究所	1	1
CNCERT 江西分中心	11	11
CNCERT 吉林分中心	3	3
CNCERT 福建分中心	1	1
CNCERT 湖北分中心	1	1
个人	7	7
报送总计	1585	669
录入总计	191（去重）	669

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Oracle、Microsoft、Adobe 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	Oracle	88	46%
2	Microsoft	31	16%
3	Adobe	29	15%
4	Cisco	12	6%
5	Juniper Networks	4	2%
6	WordPress	2	1%

7	IBM	2	1%
8	TOTOLINK	2	1%
9	Ansible	2	1%
10	其他	19	11%

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 191 个漏洞。其中应用程序漏洞 109 个，数据库漏洞 43 个，操作系统漏洞 24 个，网络设备漏洞 8 个，WEB 应用漏洞 6 个，安全产品漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	109
数据库漏洞	43
操作系统漏洞	24
网络设备漏洞	8
WEB 应用漏洞	6
安全产品漏洞	1

表 3 漏洞按影响类型统计表

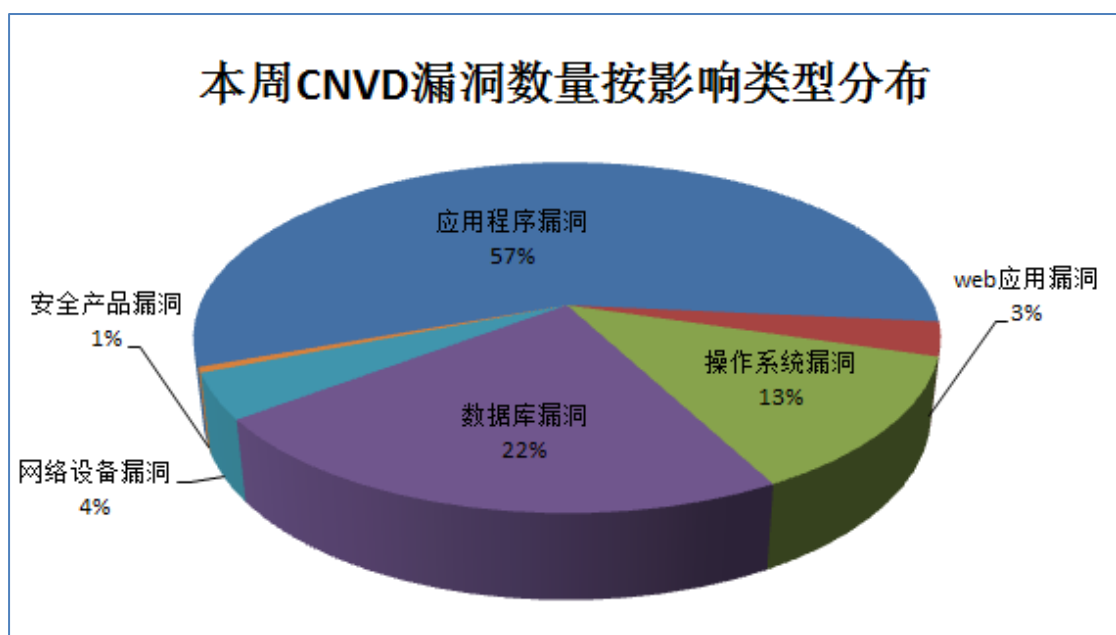


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 35 个电信行业漏洞，2 个移动互联网行业漏洞（如下图表所示）。其中，“Juniper Junos BGP-VPLS 处理拒绝服务漏洞、Juniper Junos BFD 远程拒

绝服务漏洞、Juniper Junos LAST_ACK 状态变换拒绝服务漏洞 、Oracle Fusion Oracle Endeca Information Discovery Studio 组件存在未明漏洞（CNVD-2015-04748、CNVD-2015-04747、CNVD-2015-04743、CNVD-2015-04744、CNVD-2015-04745、CNVD-2015-04746）、Oracle Fusion Oracle Data Integrator 组件存在未明漏洞（CNVD-2015-04751）、Oracle Database Java VM 组件权限提升漏洞、Grandstream GXV3275 存在多个漏洞”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-2015-04675	Cisco ASR 拒绝服务漏洞（CNVD-2015-04675）	中	是
电信	CNVD-2015-04683	Oracle MySQL Server GIS 子组件拒绝服务漏洞	中	是
电信	CNVD-2015-04684	Oracle Database Server RDBMS Support Tools 组件存在未明漏洞	低	是
电信	CNVD-2015-04692	Juniper Junos BGP-VPLS 处理拒绝服务漏洞	高	是
电信	CNVD-2015-04702	Cisco Unified Communications Manager 存在多个跨站脚本漏洞（CNVD-2015-04702）	中	是
电信	CNVD-2015-04698	Cisco Unified Communications Manager 拒绝服务漏洞（CNVD-2015-04698）	中	是
电信	CNVD-2015-04713	Juniper Junos BFD 远程拒绝服务漏洞	高	是
电信	CNVD-2015-04711	Juniper Junos LAST_ACK 状态变换拒绝服务漏洞	高	是
电信	CNVD-2015-04718	Oracle MySQL Server:Security:Firewall 组件存在未明漏洞（CNVD-2015-04718）	低	是
电信	CNVD-2015-04717	Oracle MySQL Server:Security:Firewall 组件存在未明漏洞（CNVD-2015-04717）	低	是
电信	CNVD-2015-04715	Oracle MySQL Server:Security:Privileges 组件存在未明漏洞（CNVD-2015-04715）	低	是
电信	CNVD-2015-04714	Oracle MySQL Server:Security:Privileges 组件存在未明漏洞（CNVD-2015-04714）	低	是
电信	CNVD-2015-04716	Oracle MySQL Server:Security:Firewall 组件存在未明漏洞（CNVD-2015-04716）	低	是
电信	CNVD-2015-04748	Oracle Fusion Oracle Endeca Information Discovery Studio 组件存在未明漏洞（CNVD-2015-04748）	高	是
电信	CNVD-2015-04747	Oracle Fusion Oracle Endeca Information Discovery Studio 组件存在未明漏洞（CNVD-2015-04747）	高	是

电信	CNVD-2015-04743	Oracle Fusion Oracle Endeca Information Discovery Studio 组件存在未明漏洞（CNVD-2015-04743）	高	是
电信	CNVD-2015-04744	Oracle Fusion Oracle Endeca Information Discovery Studio 组件存在未明漏洞（CNVD-2015-04744）	高	是
电信	CNVD-2015-04745	Oracle Fusion Oracle Endeca Information Discovery Studio 组件存在未明漏洞（CNVD-2015-04745）	高	是
电信	CNVD-2015-04746	Oracle Fusion Oracle Endeca Information Discovery Studio 组件存在未明漏洞（CNVD-2015-04746）	高	是
电信	CNVD-2015-04753	Oracle Fusion Oracle Data Integrator 组件存在未明漏洞（CNVD-2015-04753）	中	是
电信	CNVD-2015-04752	Oracle Fusion Oracle Data Integrator 组件存在未明漏洞（CNVD-2015-04752）	中	是
电信	CNVD-2015-04749	Oracle Fusion Oracle Data Integrator 组件存在未明漏洞（CNVD-2015-04749）	中	是
电信	CNVD-2015-04750	Oracle Fusion Oracle Data Integrator 组件存在未明漏洞（CNVD-2015-04750）	中	是
电信	CNVD-2015-04751	Oracle Fusion Oracle Data Integrator 组件存在未明漏洞（CNVD-2015-04751）	高	是
电信	CNVD-2015-04793	TOTOLINK Router Models 后门漏洞	高	否
电信	CNVD-2015-04794	TOTOLINK Router Models 代码执行漏洞	高	否
电信	CNVD-2015-04811	Oracle Database Core RDBMS 组件存在未明漏洞（CNVD-2015-04811）	中	是
电信	CNVD-2015-04810	Oracle Database Application Express 组件存在未明漏洞（CNVD-2015-04810）	中	是
电信	CNVD-2015-04805	Oracle Database RDBMS Security 组件存在未明漏洞	中	是
电信	CNVD-2015-04809	Oracle Database Application Express 组件存在未明漏洞（CNVD-2015-04809）	中	是
电信	CNVD-2015-04806	Oracle Database RDBMS Scheduler 组件存在未明漏洞	中	是
电信	CNVD-2015-04808	Oracle Database Application Express 组件存在未明漏洞（CNVD-2015-04808）	低	是
电信	CNVD-2015-04807	Oracle Database Java VM 组件权限提升漏洞	高	是
电信	CNVD-2015-04813	Oracle Database Oracle OLAP 组件存在未明漏洞（CNVD-2015-04813）	中	是
电信	CNVD-2015-04812	Oracle Database RDBMS Partitioning 组件存在未明漏洞	中	是
移动互联网	CNVD-2015-04694	Grandstream GXV3275 存在多个漏洞	高	是

移动互联网	CNVD-2015-04758	Oracle Virtualization Secure Global Desktop 组件漏洞	中	是
-------	-----------------	--	---	---

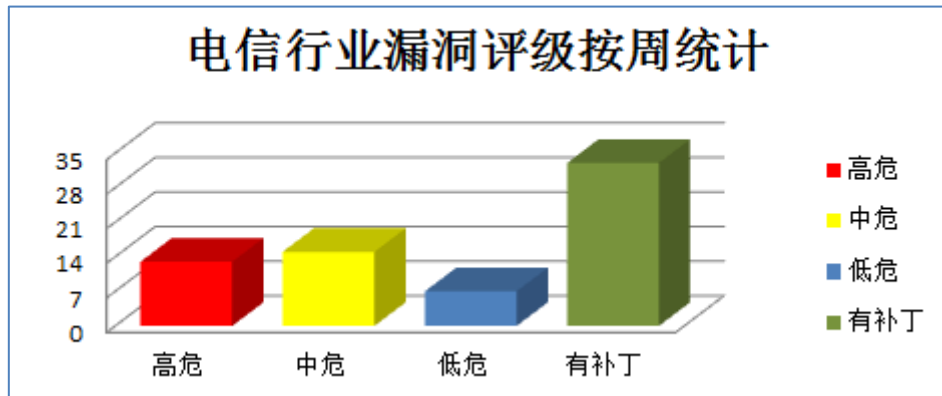


图 1 电信行业漏洞统计

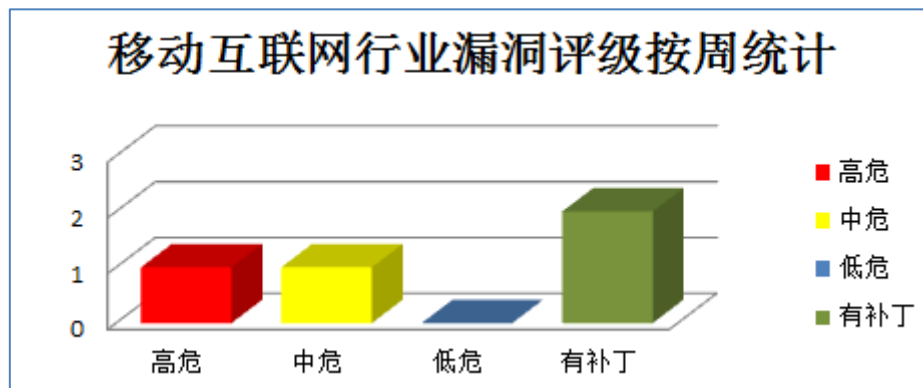


图 2 移动互联网行业漏洞统计

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、Oracle 产品安全漏洞

7 月 17 日，Oracle 发布了 2015 年 7 月份的安全更新，修复了其多款产品存在的 193 个安全漏洞。受影响的产品包括 Oracle 数据库（10 个）、中间件产品 Fusion Middleware（39 个）；企业管理器网格控制产品 Oracle Enterprise Manager Grid Control（3 个）、电子商务套装软件 Oracle E-Business Suite（13 个）、供应链套装软件 Oracle Supply Chain Products Suite（7 个）、Oracle Siebel 托管型 CRM 软件（5 个）；Hyperion（4 个）、PeopleSoft 产品（8 个）、Commerce Platform（2 个）、Industry Applications（2 个）、Virtualization（11 个）、Berkeley DB（25 个）；Java SE（25 个）、Oracle Sun 系统产品（21 个）和 MySQL 数据库（18 个）。本次安全更新提供了针对 42 个高危漏洞的补丁，有 149 个漏洞可被远程利用。

CNVD 收录的相关漏洞包括：Oracle Fusion Oracle Endeca Information Discovery

Studio 组件存在未明漏洞 (CNVD-2015-04743、CNVD-2015-04744、CNVD-2015-04745、CNVD-2015-04746、CNVD-2015-04747、CNVD-2015-04748)、Oracle Fusion Oracle Data Integrator 组件存在未明漏洞 (CNVD-2015-04751)、Oracle Sun Systems Products Suite Solaris 组件任意代码执行漏洞。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/webinfo/show/3665>

2、Microsoft 产品安全漏洞

Microsoft Windows Server 是美国微软 (Microsoft) 公司推出的一系列基于 windows 操作系统的服务器。本周, 上述产品被披露存在权限提升和任意代码执行漏洞。攻击者可利用漏洞提升权限或获执行任意代码。

CNVD 收录的相关漏洞包括: Microsoft Windows Server 权限提升漏洞 (CNVD-2015-04666、CNVD-2015-04661、CNVD-2015-04662、CNVD-2015-04663、CNVD-2015-04665)、Microsoft Windows Server 任意代码执行漏洞、Microsoft Windows 任意代码执行漏洞、Microsoft Windows 权限提升漏洞 (CNVD-2015-04691)。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-2015-04666>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04661>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04662>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04663>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04665>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04668>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04672>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04691>

3、Adobe 产品安全漏洞

Adobe Reader Acrobat 是美国 Adobe 公司开发的非常流行的一款优秀的 PDF 文档阅读软件。本周, 上述产品被披露存在限制绕过漏洞。攻击者可利用漏洞绕过限制, 执行未授权操作。

CNVD 收录的相关漏洞包括: Adobe Reader/Acrobat JavaScript API 执行限制绕过漏洞 (CNVD-2015-04646、CNVD-2015-04647、CNVD-2015-04648、CNVD-2015-04649、CNVD-2015-04650、CNVD-2015-04651、CNVD-2015-04652、CNVD-2015-04653)。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-2015-04646>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04647>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04648>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04649>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04650>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04651>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04652>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04653>

4、Cisco 产品安全漏洞

Cisco ASR 5000 和 5500 device 是思科公司的 5000 系列无线控制器产品。Cisco Unified Communications Manager 是一款 Cisco IP 电话解决方案中的呼叫处理组件。Cisco WebEx Meeting Center 是一套 WebEx 会议解决方案中的网络在线会议产品。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。Cisco FireSIGHT 管理中心可以集中式管理采用 FirePOWER Services 的 Cisco ASA 和思科 FirePOWER 网络安全设备的网络安全和运行功能。本周，上述产品被披露存在命令执行、跨站脚本、跨站请求伪造和拒绝服务漏洞。攻击者可利用漏洞执行 Linux 命令、进行跨站脚本和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 ASR 任意的 Linux 命令执行漏洞、Cisco Unified Communications Manager 拒绝服务漏洞（CNVD-2015-04698）、Cisco WebEx Meeting Center 存在多个跨站脚本漏洞（CNVD-2015-04700）、Cisco Unified Communications Manager 存在多个跨站脚本漏洞（CNVD-2015-04702）、Cisco Identity Services Engine 存在多个跨站脚本漏洞（CNVD-2015-04709）、Cisco FireSIGHT System Software 存在多个跨站脚本漏洞、Cisco ASR 拒绝服务漏洞（CNVD-2015-04675）、Cisco Identity Services Engine 跨站请求伪造漏洞。其中，“Cisco ASR 任意的 Linux 命令执行漏洞”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-2015-04696>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04698>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04700>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04702>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04709>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04712>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04675>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04673>

5、TOTOLINK Router Models 后门漏洞

TOTOLINK 生产路由器，无线接入点和网络设备。本周，TOTOLINK 被披露存在

综合评级为“高危”的后门漏洞。攻击者利用该漏洞可绕过认证系统，执行任意代码。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-2015-04793>

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-2015-04655	Adobe Reader/Acrobat 堆缓冲区溢出漏洞（CNVD-2015-04655）	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://helpx.adobe.com/security/products/reader/apsb15-15.html
CNVD-2015-04645	Adobe Reader/Acrobat 内存错误引用漏洞（CNVD-2015-04645）	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://helpx.adobe.com/security/products/reader/apsb15-15.html
CNVD-2015-04638	Adobe Reader/Acrobat 缓冲区溢出漏洞（CNVD-2015-04638）	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://helpx.adobe.com/security/products/reader/apsb15-15.html
CNVD-2015-04697	多个 VMware 产品 Host 权限提升漏洞	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.nettitude.co.uk/vmware-multiple-products-privilege-escalation/
CNVD-2015-04733	Siemens SIPROTEC 4 拒绝服务漏洞	高	厂商已提供固件更新 V4.25 EN100 模块修复漏洞： http://www.siemens.com/downloads/siprotec-4
CNVD-2015-04739	Sysphonic Thetis SQL 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： http://sysphonic.com/en/thetis/THETIS-SEC-001.html
CNVD-2015-04742	NVIDIA GPU for FreeBSD 驱动程序漏洞	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://nvidia.custhelp.com/app/answers/detail/a_id/3693
CNVD-2015-04822	Zenphoto 存在多个未明漏洞	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.zenphoto.org/news/zenphoto-1.4.9
CNVD-2015-04824	NHN Japan LINE@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这个安全问题，请到厂商的主页下载： http://official-blog.line.me/ja/archives/36495925.html
CNVD-2015-04828	Ansible 安全绕过漏洞	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://releases.ansible.com/ansible/

表 3 部分高危漏洞列表

小结：7月17日，Oracle 发布了 2015 年 7 月份的安全更新，修复了其多款产品存在的 193 个安全漏洞。此外，Microsoft、Cisco、Adobe 多款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、提升权限、执行任意代码、绕过安全限制、进行跨站脚本和跨站请求伪造攻击或发起拒绝服务攻击。另外，TOTOLINK 被披露存在一个高危零日漏洞，攻击者利用该漏洞可绕过认证系统，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、WordPress 修补 Paid Memberships Pro /Count Per Day 插件漏洞

WordPress 是一种使用 PHP 语言开发的博客平台，用户可以在支持 PHP 和 MySQL 数据库的服务器上架设属于自己的网站。

本周，WordPress 修补了上述产品存在的跨站脚本和 SQL 注入漏洞，避免攻击者利用漏洞进行跨站脚攻击或获得敏感信息。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/61371>
<http://www.cnvd.org.cn/patchInfo/show/61366>

本周要闻速递

1. WordPress 曝 XSS 高危漏洞，影响上百万网站

WordPress 团队于周二在其博客中写道，WordPress 4.2.3 版本修复了一个跨站脚本（XSS）漏洞，拥有作者权限、投稿者权限的用户都可以利用该漏洞入侵网站。攻击者可以利用该漏洞在 web 应用程序中嵌入恶意 HTML、javascript、Flash 等，绕过 wordpress 的kses 防护，然后在其系统上执行恶意脚本。执行恶意脚本不是最终目的，搜集用户敏

感信息才是初衷，在恶意脚本执行之后，系统上存储的 cookies 都会被攻击者窃取。然而 wordpress 公司并没有公布具体的漏洞细节。

参考链接: <http://www.freebuf.com/news/73139.html>

2. OpenSSH 曝高危漏洞，Linux 主机面临暴力破解威胁

OpenSSH 曝高危漏洞，Linux 主机面临暴力破解威胁。OpenSSH 是最流行的 Linux 系统进行远程控制的软件。一般来说，软件允许 3 到 6 次的密码登陆尝试，然后就会关闭连接。但是这个新爆出的漏洞会允许攻击者执行大量的登录尝试。一位网名 KingCope 的安全研究人员在博客中写道，对于使用键盘交互认证模式的 OpenSSH 服务器，包括 FreeBSD Linux，黑客都可以实施暴力破解。

参考链接: <http://www.freebuf.com/news/73132.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