

信息安全漏洞周报

2016 年 01 月 18 日-2016 年 01 月 24 日

2016年第4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 165 个，其中高危漏洞 56 个、中危漏洞 96 个、低危漏洞 13 个。上述漏洞中，可利用来实施远程攻击的漏洞有 137 个。本周收录的漏洞中，已有 154 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“mcc art.xls Bitrix 模块存在多个 SQL 注入漏洞”、“Digital Electronics Proface GP-Pro EX 任意代码执行漏洞”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 7 家成员单位、合作伙伴及个人报送了本周收录的全部 165 个漏洞。报送情况如表 1 所示。其中，奇虎(补天平台)、启明星辰、安天实验室、天融信等单位报送数量较多。补天平台、乌云、漏洞盒子及白帽子向 CNVD 提交了 862 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)	426	426
启明星辰	285	0
安天实验室	157	0
天融信	100	0
绿盟科技	69	0
恒安嘉新	21	0

H3C	4	0
乌云	371	371
漏洞盒子	29	29
CNCERT 江西分中心	6	6
CNCERT 甘肃分中心	2	2
CNCERT 安徽分中心	1	1
CNCERT 宁夏分中心	1	1
CNCERT 天津分中心	1	1
个人	25	25
报送总计	1511	862
录入总计	165（去重）	862

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Microsoft、Huawei、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	Microsoft	23	14%
2	Huawei	18	11%
3	Adobe	11	7%
4	IBM	11	7%
5	Cisco	9	5%
6	QEMU	4	2%
7	Linux	4	2%
8	F5	4	2%
9	FreeRADIUS	3	2%
10	其他	78	48%

表 2 漏洞产品涉及厂商分布统计表

本周，CNVD 收录了 165 个漏洞。其中应用程序漏洞 99 个，网络设备漏洞 33 个，操作系统漏洞 18 个，Web 应用漏洞 13 个，安全产品漏洞 2 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	99
网络设备漏洞	33
操作系统漏洞	18
Web 应用漏洞	13
安全产品漏洞	2

表 3 漏洞按影响类型统计表

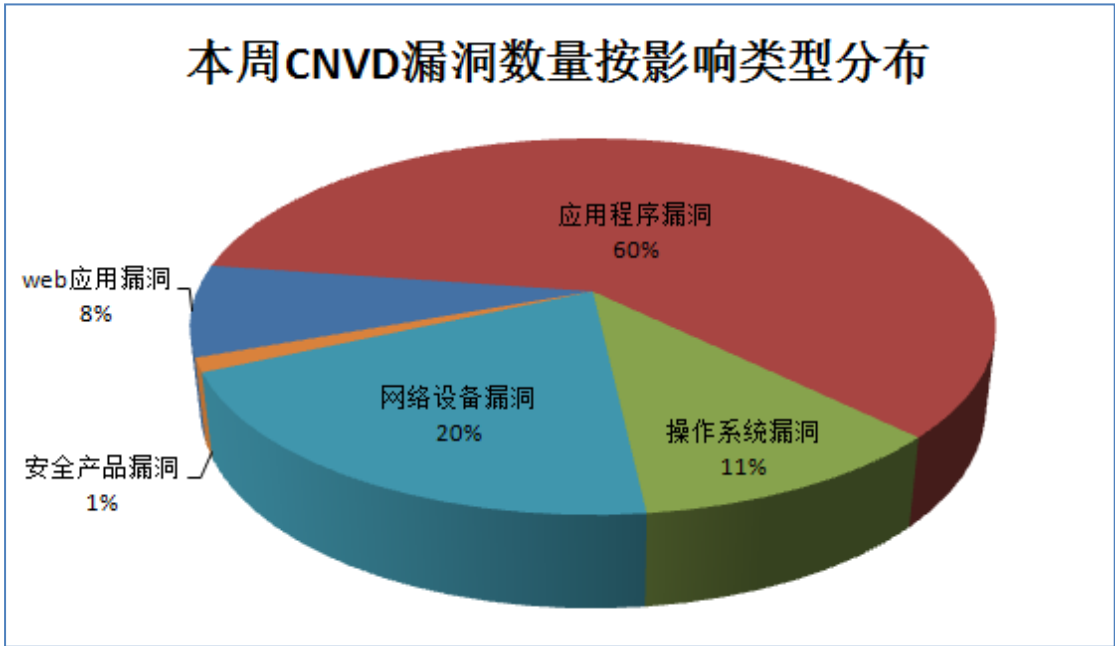


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 8 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，“Cisco Wireless LAN Controller 未授权访问漏洞、Advantech WebAccess 缓冲区溢出漏洞（CNVD-2016-00389）、Advantech WebAccess 文件上传漏洞”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-2016-00302	AVM FRITZ!OS 跨站脚本漏洞	中	是
电信	CNVD-2016-00307	IBM WebSphere Commerce 开放重定向个漏洞	中	是
电信	CNVD-2016-00322	IBM WebSphere Commerce 跨站请求伪造漏洞	中	是
电信	CNVD-2016-00370	Cisco Wireless LAN Controller 未授权访	高	是

		问漏洞		
电信	CNVD-2016-00361	Huawei Ethernet Switch 本地信息泄露漏洞	低	是
电信	CNVD-2016-00360	Huawei CloudEngine Series Switches 拒绝服务漏洞	中	是
电信	CNVD-2016-00375	Cisco Identity Services Engine Software 未授权访问漏洞	中	是
电信	CNVD-2016-00398	IBM WebSphere Commerce 跨站脚本漏洞	中	是
工控系统	CNVD-2016-00389	Advantech WebAccess 缓冲区溢出漏洞(CNVD-2016-00389)	高	是
工控系统	CNVD-2016-00390	Advantech WebAccess 文件上传漏洞	高	是

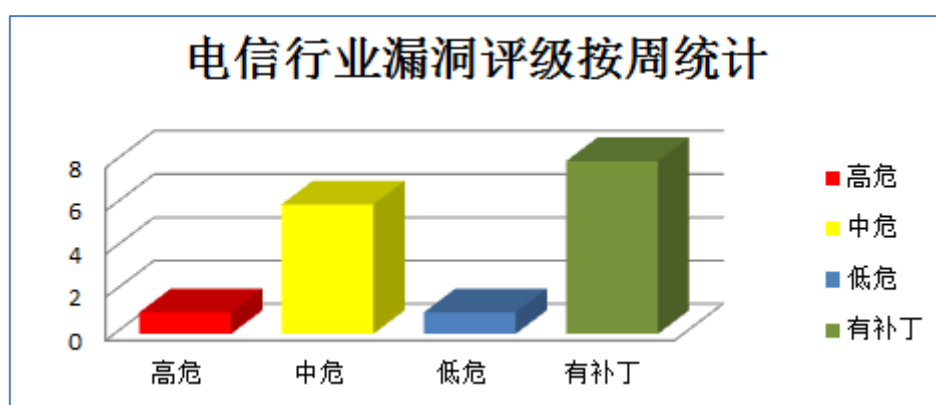


图 1 电信行业漏洞统计

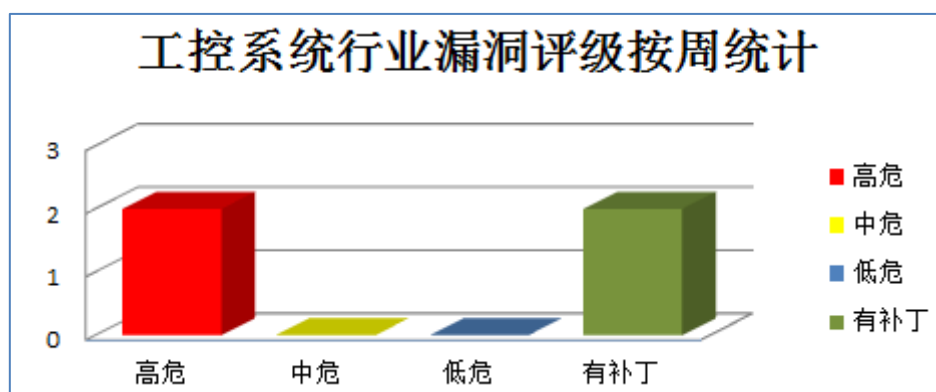


图 2 工控系统行业漏洞统计

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

Microsoft Exchange Server 是一款 Microsoft 开发的企业级的流行的邮件服务器。Microsoft Windows 是美国微软（Microsoft）公司推出的一系列为个人电脑和服务用户设计的操作系统。Microsoft Internet Explorer 是美国微软（Microsoft）公司推出的并

与 Windows 操作系统捆绑在一起的流行的 Web 浏览器。Microsoft SharePoint Server 是美国微软（Microsoft）公司推出的服务器功能集成套件，提供全面的基于 WEB 的信息共享和文档协作技术的内容管理和企业搜索，加速共享业务流程并简化跨界限信息共享。本周，上述产品被披露存在跨站脚本和安全机制绕过漏洞，攻击者利用漏洞可进行跨站脚本攻击和绕过安全限制。

CNVD 收录的相关漏洞包括：Microsoft Exchange Server 跨站脚本漏洞（CNVD-2016-00281、CNVD-2016-00280、CNVD-2016-00279、CNVD-2016-00278）、Microsoft Windows 安全机制绕过漏洞（CNVD-2016-00252、CNVD-2016-00283）、Microsoft Internet Explorer 安全机制绕过漏洞（CNVD-2016-00287）、Microsoft SharePoint Server 安全机制绕过漏洞。其中，“Microsoft Windows 安全机制绕过漏洞（CNVD-2016-00283）”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-2016-00281>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00280>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00279>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00278>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00252>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00283>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00287>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00291>

2、Adobe 产品安全漏洞

Adobe Reader 是一款 PDF 文档阅读软件。Acrobat 是 PDF 文档编辑软件。本周，上述产品被披露存在内存破坏和内存错误引用漏洞，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 Reader 及 Acrobat 内存破坏漏洞（CNVD-2016-00262、CNVD-2016-00263、CNVD-2016-00264、CNVD-2016-00265、CNVD-2016-00266、CNVD-2016-00267）、Adobe Reader 及 Acrobat 内存错误引用漏洞（CNVD-2016-00268、CNVD-2016-00270）。其中，除“Adobe Reader 及 Acrobat 内存错误引用漏洞（CNVD-2016-00268、CNVD-2016-00270）、Adobe Reader 及 Acrobat 内存破坏漏洞（CNVD-2016-00265）”外，其余漏洞的综合评级均为“高危”。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-2016-00262>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00263>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00264>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00265>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00266>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00267>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00268>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00270>

3、Huawei 产品安全漏洞

Huawei P8 及 Huawei Smart Phones 7 是中国华为公司的一款智能手机。本周，上述产品被披露存在本地权限提升、缓冲区溢出和拒绝服务漏洞，攻击者利用漏洞可提升权限和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Huawei P8 本地权限提升漏洞、Huawei P8 本地权限提升漏洞（CNVD-2016-00341、CNVD-2016-00340、CNVD-2016-00339、CNVD-2016-00342）、Huawei P8 HIFI 驱动程序缓冲区溢出漏洞、Huawei Smart Phones 本地提权漏洞、Huawei Smart Phones 本地拒绝服务漏洞。其中，除“Huawei Smart Phones 本地拒绝服务漏洞”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-2016-00343>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00341>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00340>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00339>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00342>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00297>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00345>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00337>

4、Cisco 产品安全漏洞

Cisco FireSIGHT Management Center 可以集中管理 Cisco ASA with FirePOWER Services 及 Cisco FirePOWER 设备的网络安全及操作功能。Cisco ASA 5500 系列自适应安全设备是用于提供安全和 VPN 服务的模块化平台，可提供防火墙、IPS、anti-X 和 VPN 服务。Cisco Adaptive Security Appliances 是美国思科公司的一套防火墙设备。该设备还包括 IPS、SSL VPN、IPSec VPN、反垃圾邮件等功能。Cisco Identity Services Engine 是美国思科公司的一款基于身份的环境感知平台。Cisco Aironet 1800 Series Access Point 是中小型无线网络接入点产品。本周，该产品被披露存在多个安全漏洞，攻击者利用漏洞可进行跨站脚本攻击、执行未授权访问或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Cisco FireSIGHT System Software 跨站脚本漏洞（CNVD-2016-00386、CNVD-2016-00385）、Cisco Adaptive Security Appliance 信息泄露漏洞（CNVD-2016-00384）、Cisco Adaptive Security Appliance Software 安全绕过漏洞、Cisco Identity Services Engine Software 未授权访问漏洞、Cisco Aironet 1800 Series Access Point 拒绝服务漏洞、Cisco Aironet 1800 Series Access Point 默认静态帐户凭证

漏洞、Cisco Identity Services Engine 未授权访问漏洞。其中，“Cisco Aironet 1800 Series Access Point 拒绝服务漏洞、Cisco Aironet 1800 Series Access Point 默认静态帐户凭证漏洞、Cisco Identity Services Engine 未授权访问漏洞”的综合评级均为“高危”。目前，厂商已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-2016-00386>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00385>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00384>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00376>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00375>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00373>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00372>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00371>

5、Cacti SQL 注入漏洞（CNVD-2016-00352）

Cacti 是 Cacti 集团的一套开源的网络流量监测和分析工具。本周，Cacti 被披露存在 SQL 注入漏洞，攻击者可利用漏洞提交特制的 SQL 查询，操作或获取数据库数据。目前，厂商尚未发布漏洞修补程序。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-2016-00352>

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-2016-00245	SAP Afaria 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://www.sap.com
CNVD-2016-00242	Pygments 任意命令执行漏洞	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://pygments.org/
CNVD-2016-00272	Trend Micro Password Manager 存在多个漏洞	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.trendmicro.com/
CNVD-2016-00271	Adobe Download Manager 可疑搜索路径漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： https://helpx.adobe.com/security/products/acrobat/apsb16-02.html

CNVD-2016-00292	多款 F5 BIG-IP 产品安全绕过漏洞	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/k/05/sol05272632.html
CNVD-2016-00300	F5 BIG-IP APM 拒绝服务漏洞	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： https://support.f5.com/kb/en-us/solutions/public/k/43/sol43552605.html
CNVD-2016-00308	多款 VMware 产品 VMware Tools HGFS 组件权限提升漏洞	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： http://www.vmware.com/security/advisories/VMSA-2016-0001.html
CNVD-2016-00312	Fortinet FortiClient Linux SSLVPN build 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： http://www.fortiguard.com/advisory/forticlient-sslvpn-linux-client-local-privilege-escalation-vulnerability
CNVD-2016-00314	QEMU 远程代码执行漏洞（CNVD-2016-00314）	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： http://wiki.qemu.org/
CNVD-2016-00315	QEMU 'fw_cfg_write()' 函数远程代码执行漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： http://wiki.qemu.org/

表 3 部分高危漏洞列表

小结：本周，Microsoft 多款产品被披露存在跨站脚本和安全机制绕过漏洞，攻击者利用漏洞可进行跨站脚本攻击和绕过安全限制。此外，Adobe、Huawei、cisco 等多款产品被披露存在多个安全漏洞，攻击者利用漏洞可提升权限、进行未授权访问、执行任意代码和发起拒绝服务攻击等。此外，Cacti 被披露存在一个高危漏洞，攻击者可利用该漏洞提交特制的 SQL 查询，操作或获取数据库数据。建议相关用户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、Joomla! 修补产品漏洞

Joomla! 是一款开放源码的内容管理系统（CMS）。

本周，Joomla! 修补了上述产品存在的 SQL 注入漏洞，避免攻击者利用漏洞执行任意 SQL 命令。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/70117>



本周要闻速递

1. 雅虎修复邮箱漏洞

目前雅虎修复了一个可被攻击者用于劫持用户邮箱的 XSS 漏洞。早前恶意攻击者可以利用该漏洞发送恶意邮件，然后就可以获取目标账户的资料以及信息。对于 XSS 跨站脚本攻击而言，可以通过来自于用户提交的文本信息来将恶意代码嵌入到可用于其他用户访问的 Web 网页中，而网站平台本身并没有对提交的文本信息进行过滤或者校验，从而被用户浏览器执行，导致 XSS 攻击。

参考链接：<http://www.freebuf.com/news/93873.html>

2. Linux 新型木马 Ekocms 出现，会截屏、录音

俄罗斯杀软厂商 Dr.Web 近日发现了 Linux 平台新型木马 Linux.Ekocms.1。从截获的木马样本来看，该木马能够截屏和录制音频文件，并发送给远程服务器。由此来看，Linux.Ekocms 是一款收集信息的木马工具，允许攻击者获取目标主机的上网行为。但目前 Dr.Web 安全专家并没有透露该木马是如何实现感染 Linux 系统用户的方式。

参考链接：<http://www.freebuf.com/news/93660.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