

信息安全漏洞周报

2016 年 09 月 19 日-2016 年 09 月 25 日

2016 年第 39 期

本周漏洞态势研判情况

本周信息安全漏洞威胁整体评价级别为**高**。

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 257 个，其中高危漏洞 146 个、中危漏洞 104 个、低危漏洞 7 个。漏洞平均分为 6.91。本周收录的漏洞中，涉及 0day 漏洞 95 个（占 37%）。其中互联网上出现“International Components for Unicode 栈缓冲区溢出漏洞、WordPress bwtf-waterquality 插件跨站脚本漏洞”等零日代码攻击漏洞，请使用相关产品的用户注意加强防范。此外，本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 892 个，与上周（512 个）环比增长 71%。

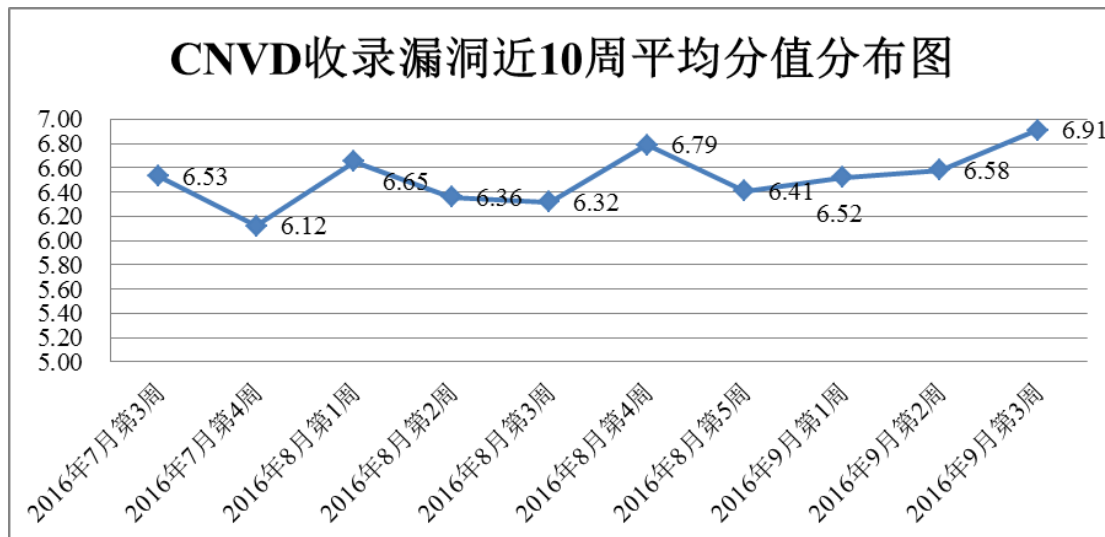


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周，共 10 家成员单位、合作伙伴及企业用户、个人用户报送了本周收录的全部 257 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、杭州安恒信息技术有限公司等单位报送数量较多。奇虎（补天平台）、漏洞盒子、腾讯玄武实验室、

南京铱迅信息技术股份有限公司、西安四叶草信息技术有限公司、新疆天山智汇信息科技有限公司、华为技术有限公司、中国航天科工四院软件评测中心、广东电网有限责任公司电力科学研究院、上海零盾网络科技有限公司、山石网科通信技术有限公司及其他个人白帽子向 CNVD 提交了 892 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）	657	657
启明星辰	222	8
安天实验室	183	0
天融信	148	0
杭州安恒信息技术有限公司	138	138
恒安嘉新	101	1
蓝盾信息安全技术有限公司	84	0
绿盟科技	62	0
中国电信集团系统集成有限责任公司	42	0
H3C	34	0
漏洞盒子	22	22
腾讯玄武实验室	2	2
南京铱迅信息技术股份有限公司	19	19
西安四叶草信息技术有限公司	16	16
新疆天山智汇信息科技有限公司	2	2
华为技术有限公司	1	1
中国航天科工四院软件评测中心	1	1
广东电网有限责任公司电力科学研究院	1	1
上海零盾网络科技有限公司	1	1

山石网科通信技术有 限公司	2	2
CNCERT 新疆分中心	3	3
CNCERT 安徽分中心	1	1
CNCERT 福建分中心	1	1
个人	16	16
报送总计	1759	892
录入总计	257（去重）	892

表 1 漏洞报送情况统计表



本周漏洞按类型和厂商统计

本周，CNVD 收录了 257 个漏洞。其中应用程序漏洞 137 个，web 应用漏洞 85 个，操作系统漏洞 18 个，网络设备漏洞 14 个，数据库漏洞 3 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	137
web 应用漏洞	85
操作系统漏洞	18
网络设备漏洞	14
安全产品漏洞	3

表 2 漏洞按影响类型统计表

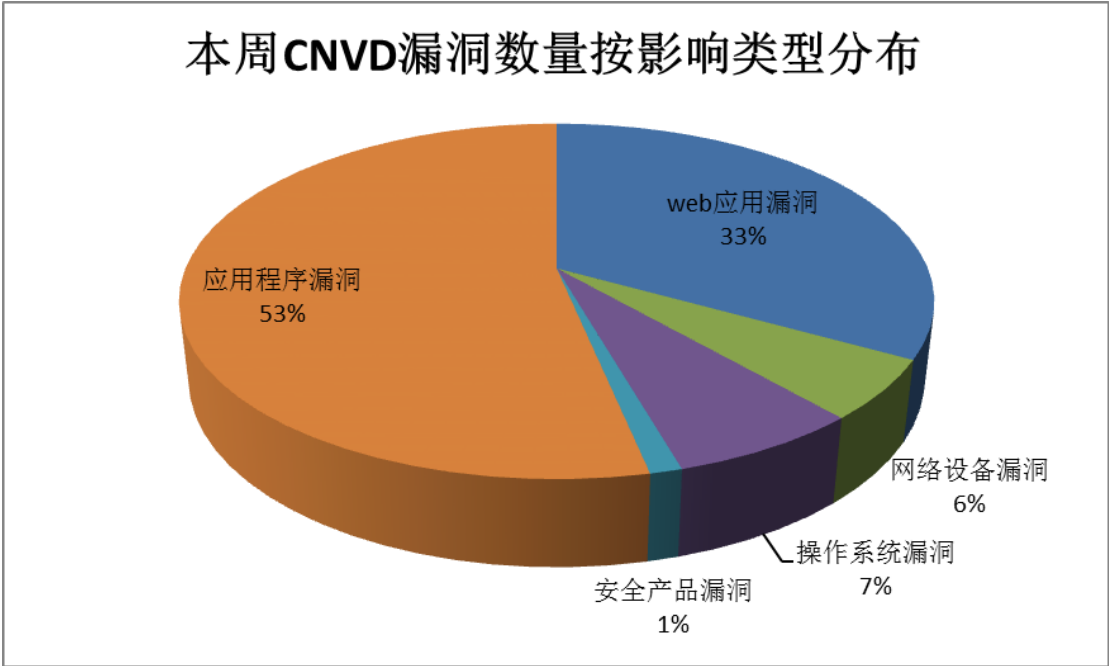


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、Microsoft、Cisco 等多家厂商的产品，部分漏洞数量按厂商统计如表 3 所示。

序号	厂商（产品）	漏洞数量	所占比例
1	Adobe	29	11%
2	Microsoft	19	7%
3	Cisco	10	4%
4	EMC	9	4%
5	IBM	9	4%
6	Wordpress	8	3%
7	VMware	8	3%
8	Apple	7	3%
9	PHP	7	3%
10	其他	151	58%

表 3 漏洞产品涉及厂商分布统计表

本周行业漏洞收录情况

本周，CNVD 收录了 9 个电信行业漏洞，11 个移动互联网行业漏洞，6 个工控系统行业漏洞（如下图所示）。其中，“Cisco WebEx Meetings Server 拒绝服务漏洞、Microsoft Silverlight 远程代码执行漏洞、ABB DataManagerPro DLL 本地代码执行漏洞、多款 Rockwell Automation 产品缓冲区溢出漏洞”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，请参照 CNVD 相关行业漏洞库链接。

电信行业漏洞链接：<http://telecom.cnvd.org.cn/>

移动互联网行业漏洞链接：<http://mi.cnvd.org.cn/>

工控系统行业漏洞链接：<http://ics.cnvd.org.cn/>

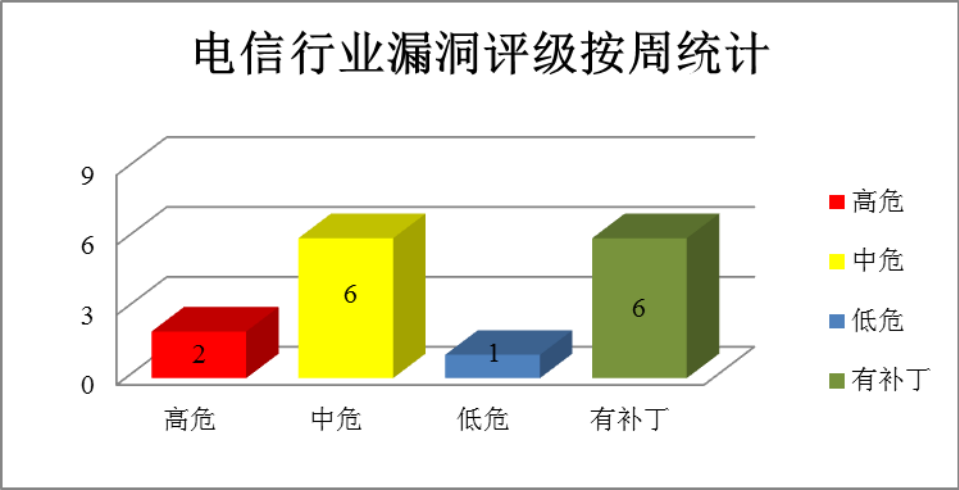


图 3 电信行业漏洞统计

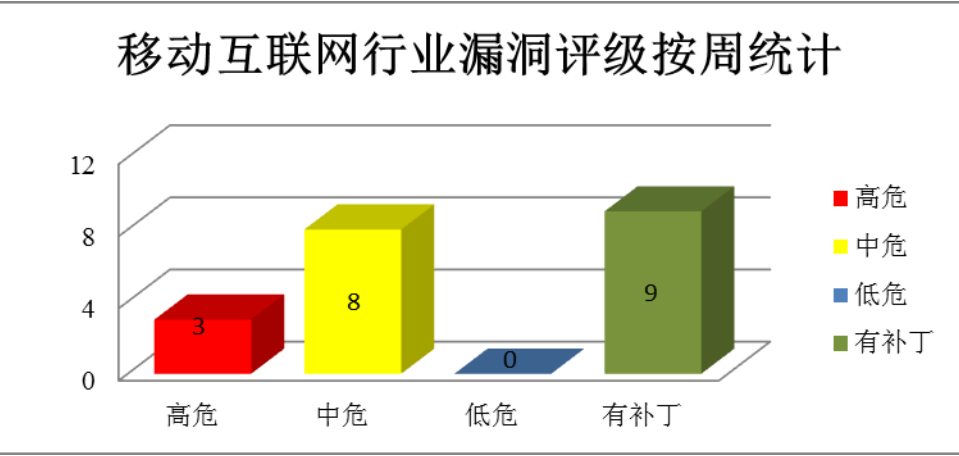


图 4 移动互联网行业漏洞统计

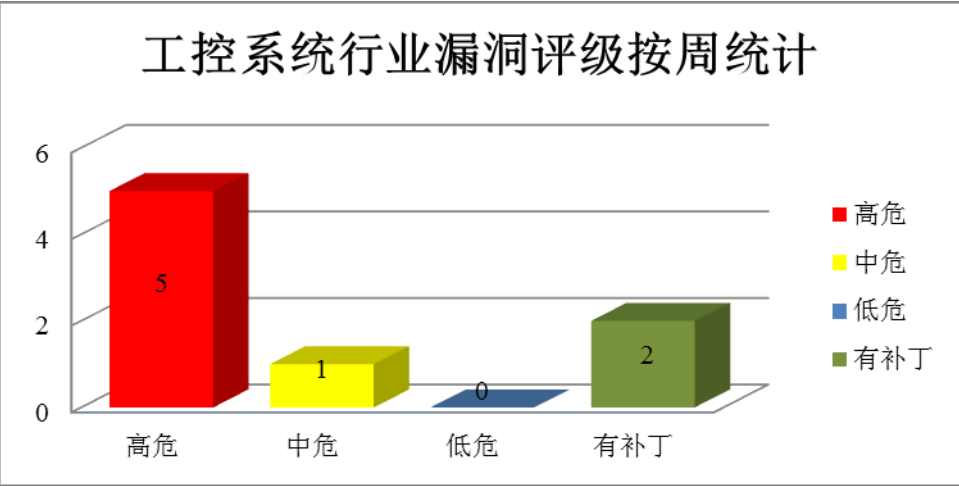


图 5 工控系统行业漏洞统计

本周重要漏洞安全告警

本周，CNVD 整理和发布以下重要安全漏洞信息。

1、Adobe 产品安全漏洞

Adobe Flash Player 是美国奥多比（Adobe）公司的一款跨平台、基于浏览器的多媒体播放器产品。本周，该产品被披露存在内存破坏漏洞，攻击者可利用该漏洞执行任意代码或造成拒绝服务（内存破坏）。

CNVD 收录的相关漏洞包括：Adobe Flash Player 内存破坏漏洞（CNVD-2016-07671、CNVD-2016-07670、CNVD-2016-07666、CNVD-2016-07675、CNVD-2016-07674、CNVD-2016-07673、CNVD-2016-07672、CNVD-2016-07676）等。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-2016-07671>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07670>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07666>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07675>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07674>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07673>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07672>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07676>

2、Microsoft 产品安全漏洞

Microsoft Windows 是美国微软（Microsoft）公司发布的一系列操作系统，Microsoft Edge 是一款 Web 浏览器，Microsoft Office 是一款办公软件套件产品。本周，上述产品被披露存多个漏洞，攻击者可利用该漏洞获取提升的权限、执行任意代码或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Microsoft Windows SMB 服务器远程代码漏洞、Microsoft Edge 脚本引擎内存破坏漏洞（CNVD-2016-07874、CNVD-2016-07815）、Microsoft Windows 本地权限提升漏洞（CNVD-2016-07746）、Microsoft Windows 远程代码执行漏洞（CNVD-2016-07747）、Microsoft Windows 拒绝服务漏洞（CNVD-2016-07748）、Microsoft Office 内存破坏漏洞（CNVD-2016-07680、CNVD-2016-07684）等。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-2016-07935>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07874>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07815>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07746>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07747>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07748>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07680>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07684>

3、Cisco 产品安全漏洞

Cisco IOS 和 IOS XE 都是美国思科（Cisco）公司为其网络设备开发的操作系统。Cisco IOS XR on NCS 6000 是一套运行于 6000 系列路由器设备中的操作系统。Cisco WebEx Meetings Server（CWMS）是一套包含音频、视频和 Web 会议的多功能会议解决方案。Cisco Unified Computing System Manager 可对统一计算系统内的所有软硬件组件提供统一的、嵌入式管理。Cisco Carrier Routing System（CRS）是一套运营商级路由系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码、获取提升的权限或进行跨站脚本攻击等。

CNVD 收录的相关漏洞包括：Cisco IOS 和 IOS XE Cisco IOx Local Manager 跨站脚本漏洞、多款 Cisco 产品信息泄露漏洞、Cisco IOS XR on NCS 6000 拒绝服务漏洞、Cisco IOS and IOS XE Data in Motion 拒绝服务漏洞、Cisco WebEx Meetings Server 拒绝服务漏洞、Cisco Unified Computing System 本地权限提升漏洞、Cisco Carrier Routing System 拒绝服务漏洞、Cisco WebEx Meetings Server 命令注入漏洞（CNVD-2016-07731）等。其中，“多款 Cisco 产品信息泄露漏洞、Cisco WebEx Meetings Server 拒绝服务漏洞”的综合评级为“高危”。目前，厂商已经发布除“Cisco Unified Computing System 本地权限提升漏洞、Cisco Carrier Routing System 拒绝服务漏洞”外漏洞的修补程序。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-2016-07871>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07726>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07727>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07725>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07722>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07728>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07729>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07731>

4、IBM 产品安全漏洞

IBM Tealeaf Customer Experience 是美国 IBM 公司的一套基于 SaaS（软件即服务）的网络和移动应用分析解决方案。IBM Rational Asset Analyzer 是一套资产分析软件。IBM WebSphere Application Server（WAS）是一款应用服务器产品。本周，上述产品被披露存在多个漏洞，攻击者可利用此漏洞泄露敏感信息、发起钓鱼攻击或进行跨站脚本攻击等。

CNVD 收录的相关漏洞包括：IBM Tealeaf Customer Experience 信息泄露漏洞、IBM Tealeaf Customer Experience 开放重定向漏洞、IBM Tealeaf Customer Experience 跨站脚本漏洞（CNVD-2016-07822）、IBM Rational Asset Analyzer 本地信息泄露漏洞、

IBM Tealeaf Customer Experience Replay Serve 存在未明漏洞、IBM Tealeaf Customer Experience 跨站脚本漏洞、IBM WebSphere Application Server Liberty 开放重定向漏洞、IBM WebSphere Application Server Liberty Profile 跨站脚本漏洞等。其中，“IBM Tealeaf Customer Experience 信息泄露漏洞、IBM Tealeaf Customer Experience 开放重定向漏洞”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-2016-07875>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07836>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07822>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07876>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07877>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07821>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07837>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07736>

5、WordPress bwtf-waterquality 插件跨站脚本漏洞

WordPress 是 WordPress 软件基金会的一套使用 PHP 语言开发的博客平台。本周，WordPress 被披露存在跨站脚本漏洞。攻击者可利用该漏洞执行跨站脚本攻击。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-2016-07662>

更多高危漏洞如表 4 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-2016-07801	Google Chrome 任意代码执行漏洞（CNVD-2016-07801）	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://googlechromereleases.blogspot.in/2016/09/stable-channel-update-for-desktop_13.html
CNVD-2016-07800	Google Chrome 任意代码执行漏洞（CNVD-2016-07800）	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://googlechromereleases.blogspot.in/2016/09/stable-channel-update-for-desktop_13.html
CNVD-2016-07805	Google Chrome Blink 内存错误引用漏洞（CNVD-2016-07805）	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://googlechromereleases.blogspot.in/2016/09/stable-channel-update-for-desktop_13.html

CNVD-2016-07804	Google Chrome Blink 内存错误引用漏洞（CNVD-2016-07804）	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://googlechromereleases.blogspot.in/2016/09/stable-channel-update-for-desktop_13.html
CNVD-2016-07803	Google Chrome V8 任意内存读取漏洞	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://googlechromereleases.blogspot.in/2016/09/stable-channel-update-for-desktop_13.html
CNVD-2016-07802	Google Chrome 任意代码执行漏洞（CNVD-2016-07802）	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://googlechromereleases.blogspot.in/2016/09/stable-channel-update-for-desktop_13.html
CNVD-2016-07811	VMware Workstation 和 Workstation Player 内存损坏漏洞	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://www.vmware.com/security/advisories/VMSA-2016-0014.html
CNVD-2016-07812	VMware Workstation 和 Workstation Player 内存损坏漏洞（CNVD-2016-07812）	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://www.vmware.com/security/advisories/VMSA-2016-0014.html
CNVD-2016-07810	VMware Workstation 和 Workstation Player 内存损坏漏洞（CNVD-2016-07810）	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://www.vmware.com/security/advisories/VMSA-2016-0014.html
CNVD-2016-07816	OpenSSL 'MDC2_Update'函数整数溢出漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页： https://www.openssl.org/

表 4 部分重要高危漏洞列表

小结：本周，Adobe 产品被披露存在内存破坏漏洞，攻击者可利用该漏洞执行任意代码或造成拒绝服务（内存破坏）。此外，Microsoft、Cisco、IBM 等多款产品被披露存在多个安全漏洞，攻击者可利用漏洞获取提升的权限、执行任意代码或进行跨站脚本攻击等。其中，思科公司披露了涉及方程式组织利用的一个高危漏洞（CNVD-2016-07726，CVE-2016-6415）。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。

本周漏洞要闻速递

1. Metasploit 曝远程代码执行漏洞：别惹我，我疯起来连自己都黑

就在本周，Rapid7 社区发布两个关于 Metasploit 框架的安全补丁，通过这两个漏洞，

攻击者可以远程非授权执行任意代码。目前，安全研究人员已经发放出相关 POC 攻击代码。Metasploit 作为一个安全测试框架，里面集成了非常多的功能，比如 msfconsole，msfvenom 等，并且也提供了非常多的接口和界面，比如 shell 接口，Windows GUI 页面，WEB UI 页面等等。而这次的问题主要是出在 WEB 接口上。MSF Community, Express 和 Pro 版本的 Web UI 在 4.12.0-2016061501 至 4.12.0-2016083001 版本中的 config.action_dispatch.cookies_serializer 值设置为 :hybrid，并且引入了 hybrid cookie 序列化，这将允许反序列化 JSON 和 Marshal 序列化的 cookies。直到 Metasploit 4.12.0-2016091401，才将其值设置为:json。也就是说，只要 cookie 序列化设置为 Marshal 或 hybrid 时，并且攻击者知道 cookie signing key 的值，那么攻击者就可以构造 cookie，触发 Marshal 反序列化，实现任意代码执行。目前这个漏洞的利用脚本已经公开到 MSF 上，模块位置是 exploit/multi/http/rails_secret_deserialization。大家可以更新自己的 MSF 使用此脚本，或者去 GitHub 上下载。

参考链接：<http://www.freebuf.com/vuls/114927.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