

信息安全漏洞周报

2016 年 10 月 24 日-2016 年 10 月 30 日

2016 年第 44 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**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 397 个，其中高危漏洞 118 个、中危漏洞 252 个、低危漏洞 27 个。漏洞平均分为 6.08。本周收录的漏洞中，涉及 0day 漏洞 72 个（占 18%）。其中互联网上出现“FreePBX 存在多个漏洞”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 786 个，与上周（1015 个）环比下降 23%。

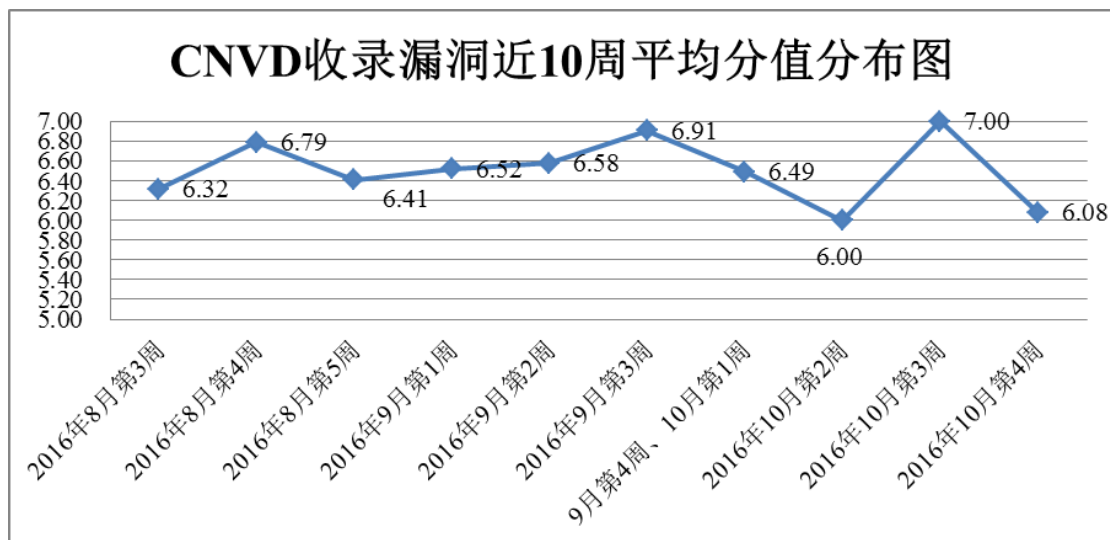


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周，共 11 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 397 个漏洞。报送情况如表 1 所示。其中，天融信、安天实验室、华为技术有限公司、启明星辰、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、广西鑫瀚科技有限公司、深圳市深信服电子科技有限公司、南京铱迅信息技术股份

有限公司、北京国舜科技股份有限公司、新疆天山智汇信息科技有限公司及其他个人白帽子向 CNVD 提交了 786 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）	613	613
天融信	221	0
安天实验室	173	0
华为技术有限公司	135	0
启明星辰	125	16
杭州安恒信息技术有限公司	92	8
H3C	90	2
恒安嘉新	74	13
蓝盾信息安全技术有限公司	71	1
中国电信集团系统集成有限责任公司	27	0
知道创宇	1	0
漏洞盒子	91	91
广西鑫瀚科技有限公司	7	7
深圳市深信服电子科技有限公司	5	5
南京铨迅信息技术股份有限公司	3	3
北京国舜科技股份有限公司	1	1
新疆天山智汇信息科技有限公司	1	1
CNCERT 山西分中心	4	4
CNCERT 宁夏分中心	2	2
CNCERT 福建分中心	2	2

CNCERT 上海分中心	1	1
个人	16	16
报送总计	1755	786
录入总计	397（去重）	786

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 397 个漏洞。其中应用程序漏洞 286 个，web 应用漏洞 57 个，数据库漏洞 34 个，网络设备漏洞 11 个，操作系统漏洞 5 个，安全产品漏洞 4 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	286
web 应用漏洞	57
数据库漏洞	34
网络设备漏洞	11
操作系统漏洞	5
安全产品漏洞	4

表 2 漏洞按影响类型统计表

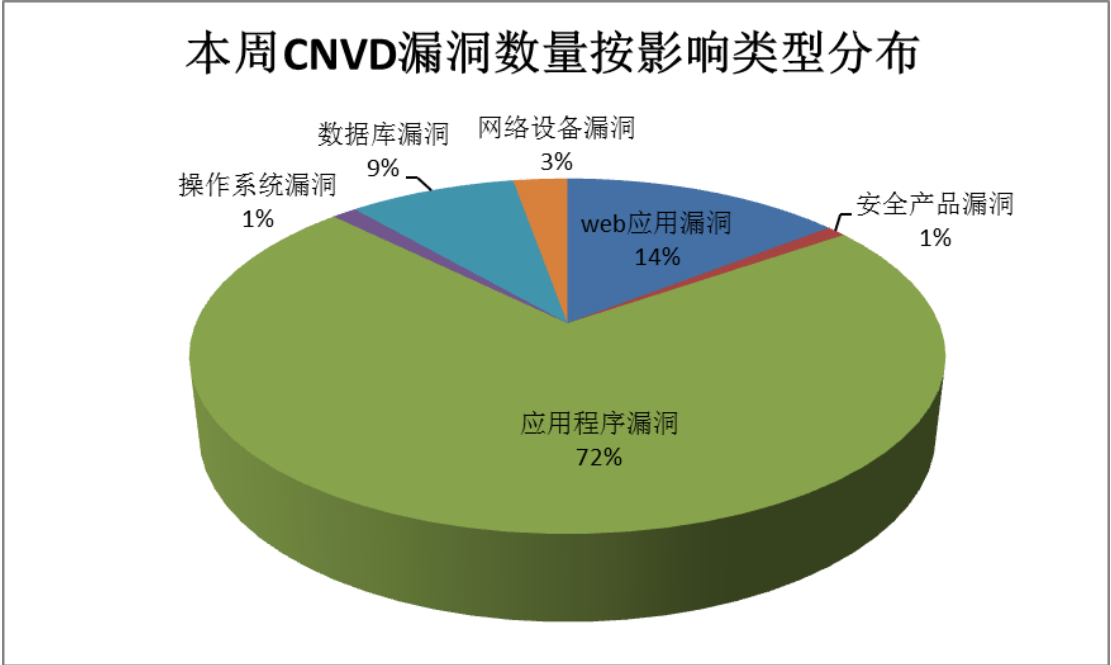


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、Wordpress、Google 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	Oracle	142	36%
2	Wordpress	21	5%
3	Google	14	4%
4	JasPer	13	3%
5	IBM	12	3%
6	potrace	11	3%
7	SAP	7	2%
8	Open-Xchange	7	2%
9	Nextcloud	5	1%
10	其他	165	41%

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 59 个电信行业漏洞，6 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，“Advantech WebAccess 8.1 ActiveX 缓冲区溢出漏洞、ADSPRPC driver for the Linux kernel 竞争条件漏洞、BlueStacks 权限提升漏洞、Clean Master 权限提升漏洞、Moxa EDR-810 路由器权限提升漏洞、Oracle Fusion Middleware Oracle Outside In Technology 组件存在未明漏洞（CNVD-2016-10068、CNVD-2016-10067、CNVD-2016-10061、CNVD-2016-10062、CNVD-2016-10063）”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/>

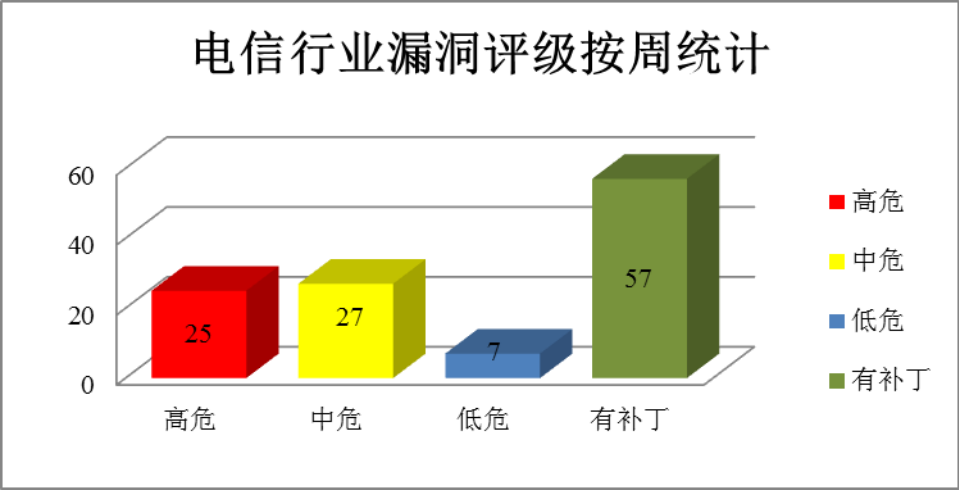


图 3 电信行业漏洞统计

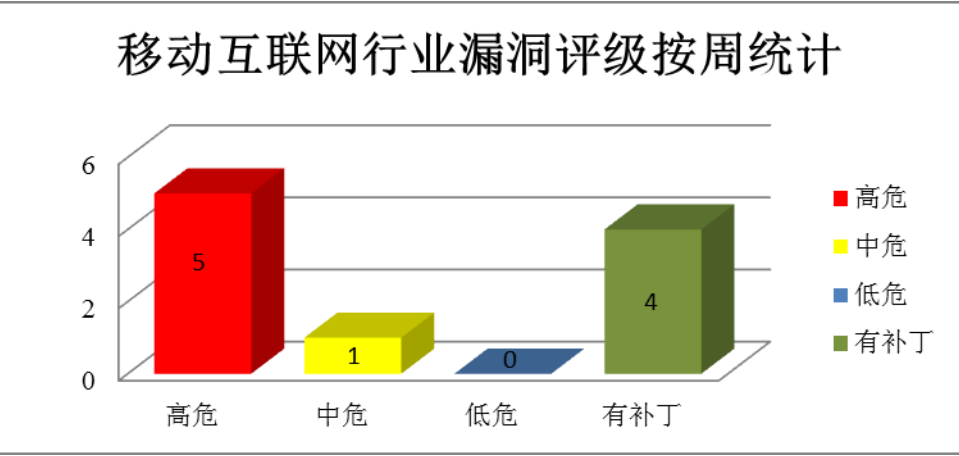


图 4 移动互联网行业漏洞统计

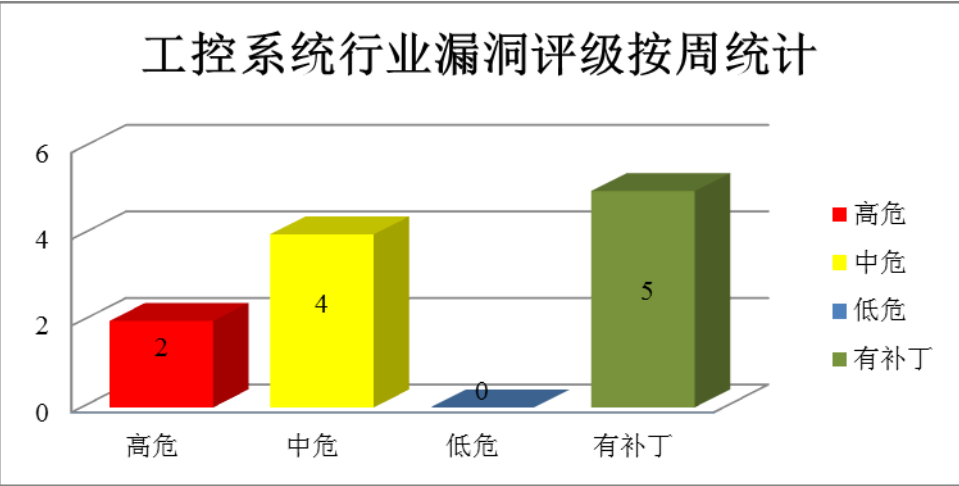


图 5 工控系统行业漏洞统计

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、Oracle 产品安全漏洞

Oracle MySQL 是美国甲骨文（Oracle）公司的一套开源的关系数据库管理系统。本周，该产品被披露存在拒绝服务漏洞，攻击者可利用漏洞发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Oracle MySQL Server 拒绝服务漏洞（CNVD-2016-09889、CNVD-2016-09890、CNVD-2016-09891、CNVD-2016-09902）、Oracle MySQL Server 组件远程拒绝服务漏洞（CNVD-2016-09885、CNVD-2016-10096、CNVD-2016-09887、CNVD-2016-09888）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-2016-09889>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-09890>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-09891>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-09902>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-09885>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10096>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-09887>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-09888>

2、Google 产品安全漏洞

Google Chrome 是一款流行的 Web 浏览器。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制、发起恶意网站 URL 欺骗或执行任意代码等。

CNVD 收录的相关漏洞包括：Google Chrome URL 欺骗漏洞（CNVD-2016-10160、CNVD-2016-10159、CNVD-2016-10158）、Google Chrome Scheme 绕过漏洞、Google Chrome Bookmarks 跨站脚本漏洞、Google Chrome Blink 跨站脚本漏洞（CNVD-2016-10245）、Google Chrome Blink 跨源绕过漏洞、Google Chrome Blink 堆溢出漏洞等。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-2016-10160>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10159>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10158>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10164>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10162>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10245>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10163>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10153>

3、IBM 产品安全漏洞

IBM Security Guardium 是美国 IBM 公司的一款数据活动监控器产品。IBM Security

ty Guardium Database Activity Monitor 是一款数据库活动监控器产品。IBM Security Guardium Database Activity Monitor 是一款数据库活动监控器产品。IBM AIX (Advanced Interactive eXecutive) 是一套 UNIX 操作系统。IBM Maximo Asset Management 是一套综合性资产生命周期和维护管理解决方案。IBM Kenexa LCMS Premier 是美国 IBM 公司的产品。本周, 上述产品被披露存在多个漏洞, 攻击者可利用漏洞泄露敏感信息、绕过安全限制或提升权限等。

CNVD 收录的相关漏洞包括: IBM Security Guardium 信息泄露漏洞、IBM TRIRIGA Application Platform 跨站脚本漏洞、IBM Jazz Foundation 信息泄露漏洞 (CNVD-2016-10072)、IBM Maximo Asset Management 信息泄露漏洞 (CNVD-2016-09860)、IBM Kenexa LCMS Premier SQL 注入漏洞、IBM Security Guardium Database Activity Monitor 存在安全绕过漏洞、IBM Security Guardium Database Activity Monitor 远程命令注入漏洞、IBM AIX 本地权限提升漏洞等。其中, “IBM Kenexa LCMS Premier SQL 注入漏洞、IBM Security Guardium Database Activity Monitor 存在安全绕过漏洞、IBM Security Guardium Database Activity Monitor 远程命令注入漏洞、IBM AIX 本地权限提升漏洞” 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-2016-10241>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10279>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10072>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-09860>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-09859>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10242>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10298>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10124>

4、SAP 产品安全漏洞

SAP BusinessObjects 是 SAP 公司旗下的商务智能产品。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。SAP SLD Registration Program (SLDREG) 是一套用于在系统架构目录中注册 SAP 系统的工具。SAP Console 是一套支持在 SAP 系统内与交换信息进行连接的分发组件。SAP SAPCRYPTOLIB 是一个密码库。本周, 上述产品被披露存在多个漏洞, 攻击者可利用漏洞泄露敏感信息、绕过安全限制或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括: SAP NetWeaver ABAP 'ST-PI'组件 SQL 注入漏洞、SAP NetWeaver ABAP 跨站脚本漏洞、SAP BusinessObjects 跨站伪造请求漏洞、SAP SLD Registration Program 拒绝服务漏洞、SAP Standalone SAPConsole 信息泄露漏洞、SAP NetWeaver 安全绕过漏洞 (CNVD-2016-09869)、SAP SAPCRYPTOLIB 组件安全绕

过漏洞。其中，“SAP NetWeaver ABAP 'ST-PI'组件 SQL 注入漏洞”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-2016-09933>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-09934>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-09935>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10043>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-09851>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-09869>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-09868>

5、Apple OS X Preview 远程代码执行漏洞

Apple OS X 是美国苹果（Apple）公司为 Mac 计算机所开发的一套专用操作系统。本周，Apple 被披露存在远程代码执行漏洞。攻击者可利用该漏洞远程执行任意代码。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-2016-10197>

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-2016-09856	ImageMagick 'coders/tiff.c' 内存泄露漏洞	高	用户可联系供应商获得补丁信息： http://www.imagemagick.org/script/index.php
CNVD-2016-09862	Project Atomic bubblewrap 本地特权提升漏洞	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.projectatomic.io/
CNVD-2016-09861	Evernote 加载远程代码执行漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： https://evernote.com/
CNVD-2016-09920	BlueStacks 权限提升漏洞	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： http://www.bluestacks.cn/
CNVD-2016-09921	Simple PHP Blog 跨站请求伪造漏洞	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： http://simpleblogphp.com/
CNVD-2016-09925	ADSPRPC driver for the Linux kernel 竞争条件漏洞	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：

			http://source.android.com/security/bulletin/2016-10-01.html
CNVD-2016-09945	Magento CMS Admin Dashboard 远程代码执行漏洞	高	目前厂商已经发布了升级版本以修复此安全问题，参考链接如下： https://magento.com/security/patches/supee-8788
CNVD-2016-09946	Hopper Disassembler 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： https://www.hopperapp.com/
CNVD-2016-09947	ImageMagick 内存破坏漏洞	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.imagemagick.org/
CNVD-2016-09995	Trend Micro 本地权限提升漏洞	高	目前厂商已经发布更新，详情请关注厂商主页或有关网址： http://www.trendmicro.com/us/index.html

表 4 部分重要高危漏洞列表

小结：本周，Oracle 被披露存在拒绝服务漏洞，允许攻击者利用漏洞发起拒绝服务攻击。此外，Google、IBM、SAP 等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、绕过安全限制、执行任意代码和发起拒绝服务攻击等。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. InTerCyber 公司在消息系统中发现了一个严重的漏洞

信息安全公司 InTheCyber 的安全研究专家发现了一个严重的漏洞，攻击者可以利用这个漏洞来伪造自己的来电显示号码，并以此来进行下一步的攻击活动，最终获取到目标用户语音信箱的访问权。这个漏洞或可影响消息系统的安全性。需要注意的是，这个漏洞的利用方法并不难。安全研究人员表示，Telegram、WhatsApp、以及 Signal 都将会受到这个漏洞的影响。

参考链接：<http://www.freebuf.com/news/117588.html>

2. AtomBombing 内存注入技术的威胁预警

在 Windows 有一个功能叫做 Atom Tables，而这个功能主要可以用于进程和进程之间的通信，线程和线程之间的通信。而 enSilo 网络安全公司的研究团队利用这个功能的设计缺陷，成功的将一个恶意代码注入到一个合法的进程当中，并且不会被杀毒软件查杀。这个缺陷影响了所有的 Windows 系统。因为它可以随意注入到任意进程，也就是说它可以注入到浏览器进程中，任意修改网页数据，达到一个中间人攻击的效果。与此同时，这个注入技术还可以获得未进行 HTTPS 加密的元数据。恶意代码可以注入到浏览器内存中，在数据传输到传输层之前将其进行截获，从而获得一份原始的未加密数据。

参考链接: <http://www.freebuf.com/news/118026.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