网络安全威胁月报 201702

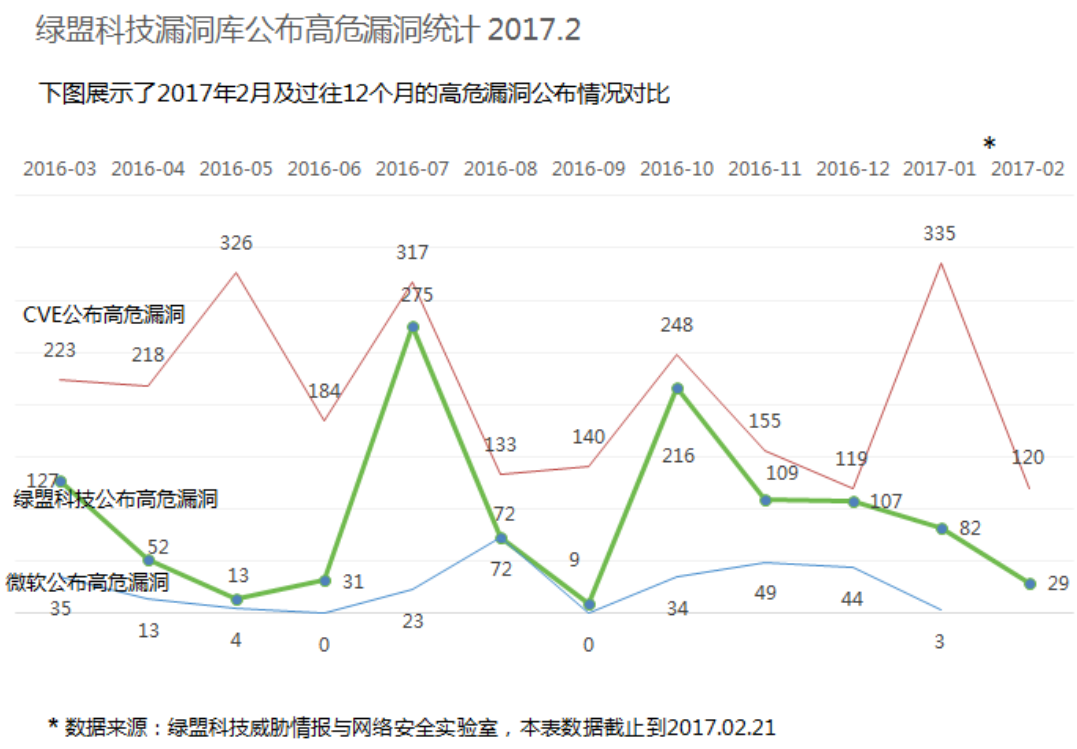
关键词 高危漏洞 DDoS 攻击事件 安全会议 绿盟科技漏洞库 绿盟科技博客

摘要 绿盟科技网络安全威胁周报及月报系列，旨在简单而快速有效的传递安全威胁态势，呈现重点安全漏洞、安全事件、安全技术。获取最新的威胁月报，请访问绿盟科技博客 http://blog.nsfocus.net/

一. 2017 年 2 月数据统计

1.1 高危漏洞发展趋势

2017 年 2 月绿盟科技安全漏洞库共收录 72 个漏洞，其中高危漏洞 29 个。相比 1 月份的高危漏洞数量有所下降。



(备注：本月微软官网漏洞延迟公布，预计 3 月份公布 2 月份补丁)

1.2 互联网安全漏洞

OpenSSL 1.1.0e 之前版本存在 CVE-2017-3733 漏洞

来源：http://toutiao.secjia.com/pls-upgrade-to-openssl-1-1-0e

简述：2017 年 2 月 16 日，OpenSSL 官网发布安全通告，公布了编号为 CVE-2017-3733 的漏洞，在 1.1.0e 之前版本的 OpenSSL 握手阶段的重协商过程中，如果协商使用 Encrypt-Then-Mac 扩展，会导致 OpenSSL 崩溃。OpenSSL 的服务端和客户端都受该漏洞的影响。

dotCMS 3.6.2 以下版本可能存在 SQL 注入漏洞

来源：http://toutiao.secjia.com/newest-dotcms-sql-injection-vulnerability

简述：2017 年 2 月 15 日，seclists.org 网站发布了关于 dotCMS 存在 SQL 注入漏洞的消息。文章称，dotCMS 3.6.1 及其之前的部分版本，在“/categoriesServlet”的 q 和 inode 参数上存在 SQL 注入，未经身份认证的攻击者可以利用该漏洞获取敏感数据。

X-Agent 间谍软件变种正在攻击 Mac 系统 据称与 APT28 有关

来源：http://toutiao.secjia.com/x-agent-spyware-variants-are-attacking-mac-systems

简述：安全研究人员发现一个新的 Mac 恶意软件，该恶意软件被设计用于窃取 web 浏览器密码，获取显示器屏幕截图，检测系统配置、执行文件，以及提取计算机上存储的 iPhone 备份文件。该间谍软件之前曾被用于对 Windows、iOS、安卓和 Linux 设备发动网络攻击。

Adobe Flash Player 存在多处漏洞

来源：http://toutiao.secjia.com/adobe-acrobat-reader-vulnerability-announcement

简述：2017 年 2 月 14 日，Adobe 官网发布漏洞安全通告，影响到 24.0.0.194 及更早版本的 Fl

ash Player，横跨 Windows、Mac、Linux 和 Chrome OS 平台。攻击者可以利用相关漏洞让目标 Flash Player 崩溃，并且有可能控制受影响的操作系统。

TP-Link C2 和 C20i 产品出现命令注入、DoS 等多个漏洞

来源：http://toutiao.secjia.com/tp-link-c2-and-c20i-vulnerability

简述：日前，pierrekim.github.io 网站发布了一个安全通告，公布了固件版本为“0.9.1 4.2 v0032.0 Build 160706 Rel.37961n”的 TP-Link C2 和 C20i 产品的多个漏洞。漏洞包括命令注入(需要身份认证)、拒绝服务以及不安全的默认配置。

WordPress 4.7.0 及 4.7.1 存在越权漏洞

来源：http://toutiao.secjia.com/wordpress-4-7-0-4-7-1-unauthorized-vulnerability

简述：在 WordPress 4.7.0-4.7.1 版本中,存在着一个越权漏洞，成功的利用这个漏洞，可以绕过管理员权限对文章进行增删改查操作。官方已经发布补丁，请广大站长朋友们尽快备份后升级。

ElasticSearch 遭遇勒索攻击

来源：http://blog.nsfocus.net/elasticsearch-suffered-blackmail-attack-analysis/

简述：春节前，有超过 34000 多台存在安全风险的 MongoDB 数据库遭到了勒索攻击，数据库数据被攻击者擦除并索要赎金，在收到赎金后攻击者才会返还服务器中的数据；紧接着，2017 年 1 月 18 日，在短短几个小时内又有数百台 ElasticSearch 服务器受到了勒索攻击，服务器中的数据被擦除，并被索要赎金。

Hadoop 遭遇勒索攻击

来源：http://blog.nsfocus.net/hadoop-suffered-blackmail-attack/

简述：最近，部分黑客组织针对几款特定产品展开了勒索攻击。

(来源：绿盟科技威胁情报与网络安全实验室)

1.3 绿盟科技漏洞库十大漏洞

NSFOCUS 2016 年 12 之十大安全漏洞
声明：本十大安全漏洞由 NSFOCUS(绿盟科技)安全小组 <security@nsfocus.com>根据安全漏洞的严重程度、利用难易程度、影响范围等因素综合评出，仅供参考。
http://www.nsfocus.net/index.php?act=sec_bug&do=top_ten

1. 2017-02-20 Windows SMBv3 远程拒绝服务漏洞
   NSFOCUS ID: 35936
   链接:http://www.nsfocus.net/vulndb/35936
   综述:Microsoft Windows 是流行的计算机操作系统。Windows Server 2012/2016、Win8/8.1 以及 Win10 系统在 SMBv3 的实现中存在远程攻击漏洞。
   危害:攻击者可以迫使受影响系统蓝屏崩溃

2. 2017-02-20 WordPress REST API 内容注入漏洞
   NSFOCUS ID: 35937
   链接:http://www.nsfocus.net/vulndb/35937
   综述:WordPress 是一种使用 PHP 语言开发的博客平台。REST API 可通过 JSON 格式传输数据访问或控制 WordPress 站点内容。WordPress REST API 插件 4.7.0 – 4.7.1 版本存在安全漏洞，此漏洞由于权限控制失效可导致内容注入或修改。
   危害:远程攻击者可以通过向服务器发送恶意请求来利用此漏洞，对服务器进行非授权的访问

3. 2017-02-15 Adobe Flash Player 类型混淆漏洞(CVE-2017-2995)
   NSFOCUS ID: 35904
   链接:http://www.nsfocus.net/vulndb/35904
   综述:Flash Player 是多媒体程序播放器。Adobe Flash Player <= 24.0.0.194 在实现上存在类型混淆漏洞，成功利用后可导致任意代码执行。
   危害:攻击者可以通过诱使受害者打开恶意 swf 文件来利用此漏洞，从而控制受害者系统

4. 2017-02-15 Oracle Java SE 远程安全漏洞(CVE-2017-3272)

NSFOCUS ID: 35902
链接:http://www.nsfocus.net/vulndb/35902
综述:Java SE 是基于 JDK 和 JRE 的 Java 平台标准版的简称，用于开发和部署桌面、服务器以及嵌入设备和实时环境中的 Java 应用程序。Oracle Java SE 6u131, 7u121, Java SE 8u111, Java SE 8u112 版本存在安全漏洞，可通过多个协议进行利用，影响 'Libraries' 子组件。
危害:远程攻击者可以利用这些漏洞控制受害者系统

5. 2017-02-06 Adobe Acrobat Reader 堆缓冲区溢出漏洞(CVE-2017-2959)
NSFOCUS ID: 35831
链接:http://www.nsfocus.net/vulndb/35831
综述:Adobe Reader 是 PDF 文档阅读软件。Adobe Acrobat Reader <=15.020.20042, <=15.006.30244, <=11.0.18 版本，在图形转换引擎中存在堆溢出漏洞，可导致任意代码执行。
危害:攻击者可以通过诱使受害者打开恶意 pdf 文件来利用此漏洞，从而控制受害者系统

6. 2017-02-10 Node.js unserialize()函数任意代码执行漏洞(CVE-2017-5941)
NSFOCUS ID: 35883
链接:http://www.nsfocus.net/vulndb/35883
综述:Node.js 是一个开放源代码、跨平台的、可用于伺服器端和网络应用的运行环境。Node.js 在 node-serialize 模块中存在安全漏洞，若 unserialize()函数输入不安全，则通过 IIFE，攻击者可执行任意代码。
危害:远程攻击者可以利用这些漏洞控制受害者系统

7. 2017-02-10 FFmpeg libavformat/rtmppkt.c 堆缓冲区溢出漏洞(CVE-2016-10191)
NSFOCUS ID: 35882
链接:http://www.nsfocus.net/vulndb/35882
综述:FFmpeg 是一个免费的可以执行音讯和视讯多种格式的录影、转档、串流功能的软件。FFmpeg < 2.8.10, 3.0.x < 3.0.5, 3.1.x < 3.1.6, 3.2.x < 3.2.2 版本，在 libavformat/rtmppkt.c 中存在堆缓冲区溢出漏洞。
危害:攻击者可以通过诱使受害者打开恶意视频文件来利用此漏洞，从而控制受害者系统

8. 2017-02-07 Google Android Audioserver 权限提升漏洞(CVE-2017-0384)
NSFOCUS ID: 35862
链接:http://www.nsfocus.net/vulndb/35862
综述:Google Chrome 是由 Google 开发的一款 Web 浏览工具。Android 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1 版本，Audioserver/libeffects/lvm/wrapper/Bundle/EffectBundle.cpp 存在权限提升漏洞。

危害:本地应用可以在特权进程上下文中执行任意代码

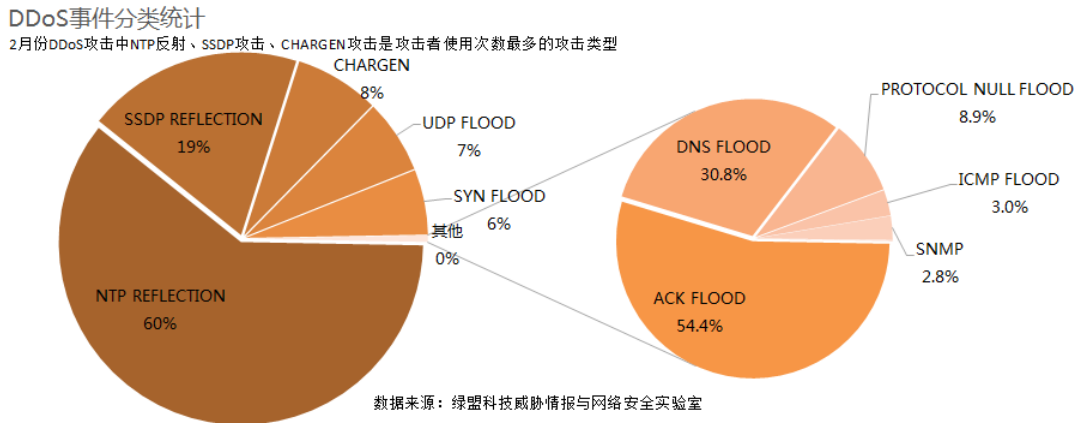
9. 2017-02-14 QEMU 'hw/display/cirrus_vga.c'远程代码执行漏洞(CVE-2017-2615)
   NSFOCUS ID: 35899
   链接:http://www.nsfocus.net/vulndb/35899
   综述:QEMU 是一款开源模拟器软件。QEMU 若支持 Cirrus CLGD 54xx VGA 模拟器，则在反向模式中，通过位块传送复制 VGA 数据中存在安全漏洞，可导致越界内存访问，造成信息泄露或权限提升。
   危害:本地攻击者可以利用此漏洞对宿主机进行非授权的访问

10. 2017-02-08 Linux Kernel 远程缓冲区溢出漏洞(CVE-2017-5577)
    NSFOCUS ID: 35864
    链接:http://www.nsfocus.net/vulndb/35864
    综述:Linux Kernel 是 Linux 操作系统的内核。Linux kernel < 4.9.7 版本，VideoCore DRM 驱动程序中 drivers/gpu/drm/vc4/vc4_gem.c/vc4_get_bcl 函数存在安全漏洞。
    危害:本地攻击者可以利用此漏洞来提升权限，对系统进行非授权的访问。

(来源：绿盟科技威胁情报与网络安全实验室)

1.4 DDoS 攻击类型

2 月份绿盟科技科技威胁情报及网络安全实验室收集及梳理了超过 15.1 万次攻击，与 1 月份相比，攻击次数略有上升，在这个月的攻击类型中，最常见的类型仍然是，SSDP,NTP,CHARGEN,UDP, SYN 这几种，ACK 攻击比例比前期明显下降。



小提示

- Chargen Flood：Chargen 字符发生器协议（Character Generator Protocol）是一种简单网络协议，设计的目的是用来调试 TCP 或 UDP 协议程序、测量连接的带宽或进行 QoS 的微调等。但这个协议并没有严格的访问控制和流量控制机制。流量放大程度在不同的操作系统上有所不同。有记录称，这种攻击类型最大放大倍数是 358.8 倍。
- NTP Flood：又称 NTP Reply Flood Attack，是一种利用网络中时间服务器的脆弱性（无认证，不等价数据交换，UDP 协议），来进行 DDoS 行为的攻击类型。有记录称，这种攻击类型最大放大倍数是 556.9 倍。
- SSDP Flood：智能设备普遍采用 UPnP（即插即用）协议作为网络通讯协议，而 UPnP 设备的相互发现及感知是通过 SSDP 协议（简单服务发现协议）进行的。

  攻击者伪造了发现请求，伪装被害者 IP 地址向互联网上大量的智能设备发起 SSDP 请求，结果被害者就收到了大量智能设备返回的数据，被攻击了。有记录称，这种攻击类型最大放大倍数是 30.8 倍。

  更多相关信息，请关注绿盟科技 DDoS 威胁报告。

二. 博文精选

RSA 会议主题回顾

RSA2017 创新沙盒冠军 unifyid

2017 年 RSA 大会的创新沙盒在选出的十家短名单的基础上，经过激烈的演讲问答环节，选出了最后的获胜者 UNIFYID。

http://blog.nsfocus.net/rsa2017-innovation-sandbox-champion-unifyid/

勒索软件防御领域

DATA，2017 年 USA RSA 会议最热门词（参见下图）。每年 RSA 会议的热门词会由组委会根据参会组织所属领域、发言人提报议题内容，包含最多的领域提炼出来。DATA、CLOUD、THREAT、INTELLIGENCE 等一直是近几年的热点领域，今年 DATA

一跃成为最热门领域。提到 DATA，既有利用大数据的 SIEM，又有数据的安全防护，还有进行广泛数据分析的 INTELLGENCE,而今年最重要的是多了一大热点——Ransomware（勒索软件）
http://blog.nsfocus.net/extreme-blackmail-software-ransomware-defense-field/

RSA2017 云安全见闻
RSA 大会开始的第一天迎来了三个 seminar，其中要数 CSA 的最为引人关注，从等候者进入大门的排队之长可见一斑
http://blog.nsfocus.net/rsa2017-cloud-security-knowledge/

金融行业安全月刊 201701 期
绿盟科技发布金融行业安全月刊 201701 期，该月刊为绿盟科技金融事业部主办的面向金融行业客户的信息安全类刊物。安全月刊分政策解读、行业研究、漏洞聚焦以及产品动态 4 个栏目，主要介绍最新安全动态、国家及行业政策（要求）落地指导、前沿技术以及安全解决方案等内容。
http://blog.nsfocus.net/financial-sector-safety-monthly-201701/

攻守"军备竞赛" 2017 如何布局
有朋友说，2016 是"突飞猛进"的一年。的确，一方面，网络攻击事件的规模和影响产生了一系列新的记录。如图 1，数据泄露单事件丢失的记录数量创出新高[1]；绿盟科技在 2016 年 8 月观察到拒绝服务攻击峰值流量达到前所未有的 3.7Tbps。
http://blog.nsfocus.net/arrange-offense-defense-s-arms-race/

（来源：绿盟科技博客）

三. 安全会议

安全会议是从近期召开的若干信息安全会议中选出，仅供参考。

CanSecWest

时间：March 15 - 17, 2017

简介: CanSecWest, the world's most advanced conference focusing on applied digital security, is about bringing the industry luminaries together in a relaxed

environment which promotes collaboration and social networking.

网址：https://cansecwest.com/

Pen Test Austin 2017

时间：Mar 27, 2017 - Sat, Apr 1, 2017

简介：Penetration Testing, Ethical Hacking, and Exploit Development training is coming to Austin, TX from SANS Institute, the global leader in information security training.

网址：https://www.sans.org/event/pentest2017