
# 绿盟科技互联网安全威胁周报 (alpha版)

# ——第201902周

## 一. 互联网安全威胁态势

### 1.1 CVE统计


最近一周CVE公告总数与前期相比有明显下降。

### 1.2 威胁信息回顾

- 标题：微软发布1月补丁修复51个安全问题

    - 时间：2019-01-09
    - 简介：本月微软修复日共修复了 51 个漏洞，有一些严重漏洞影响到 Edge、Hyper-V 和 DHCP 等产品。微软表示本次修复的漏洞都没有利用实例，但其中编号为 CVE-2019-0579 的漏洞曾被公开披露过，主要影响 Windows Jet 数据库引擎。与此同时，Adobe 也发布了漏洞补丁，主要解决了 Connect 和 Digital Editions 中的两个“重要”漏洞。
    - 链接：http://blog.nsfocus.net/microsoft-released-a-january-patch-to-fix-51-security-issues/

- 标题：与伊朗有关的APT组织支持全球DNS劫持活动
    - 时间：2019-01-11
    - 简介：近日，一些安全研究人员对劫持域名的DNS攻击发出了警告，称攻击规模史无前例。攻击者能够通过DNS劫持收集到用户名和密码，而终端用户对此几乎一无所知。目前，研究人员称攻击者主要针对北美、欧洲、中东和北非实体的域名，认为攻击者可能与伊朗的APT组织有关。
    - 链接：https://securityaffairs.co/wordpress/79722/apt/iran-apts-dns-hijacking.html
- 标题：TA505组织采用新的ServHelper后门和FlawedGrace远程木马进行攻击
    - 时间：2019-01-10
    - 简介：由TA505网络犯罪团伙通过网络钓鱼活动分发了两个新的恶意软件系列：ServHelper后门有两个变种和FlawedGrace远程访问木马（RAT）。近期攻击者瞄准金融和零售行业的组织，使用Microsoft Word，Microsoft Publisher和PDF文件诱导受害者主机感染恶意软件。
    - 链接：https://www.bleepingcomputer.com/news/security/ta505-group-adopts-new-servhelper-backdoor-and-flawedgrace-rat/
- 标题：泄露数百名德国政客信息的黑客被捕
    - 时间：2019-01-08
    - 简介：近期有报道称德国多名政客信息泄露，连德国总理默克尔也未能幸免。当时泄露的信息包括邮箱地址、手机号、收据、身份文件复印件以及个人聊天记录等。目前，外媒报道称涉事的黑客已经被逮捕且已经认罪。
    - 链接：https://securityaffairs.co/wordpress/79653/data-breach/german-politicians-leak-culprit.html
- 标题：Ryuk勒索软件和TrickBot结合获得对受感染网络的访问权限
    - 时间：2019-01-12
    - 简介：Ryuk被认为是一种有针对性的勒索软件，可以通过远程桌面服务或其他直接方法获取目标主机访问权限，窃取凭据，然后针对数据和服务器勒索可能的最高赎金金额。近期，Ryuk和TrickBot结合被用于攻击影响华尔街日报，纽约时报和洛杉矶时报等大型出版物的报纸发行。
    - 链接：https://www.bleepingcomputer.com/news/security/ryuk-ransomware-partners-with-trickbot-to-gain-access-to-infected-networks/
- 标题：Dark Overlord组织放出第一批650份机密级9/11事件文件的解密密钥
    - 时间：2019-01-07
    - 简介：近日，Dark Overlord黑客组织声称从英国保险公司Hiscox窃取了大量9/11事件相关的

机密文件。2018年4月，Hiscox承认数据泄露，并确认被黑客入侵的服务器“可能包含了有关多达1,500名Hiscox美国商业保险保单持有人的信息。”2018年12月31日，保险公司确认被盗文件包括有关9/11事件的信息。

- 链接：https://securityaffairs.co/wordpress/79549/hacking/the-dark-overlord-9-11.html?tdsourcetag=s_pctim_aiomsg

- 标题：GoDaddy被发现将JavaScript注入其在托管的网站的所有网页
  - 时间：2019-01-13
  - 简介：知名域名注册、主机服务网站GoDaddy被发现其在托管的网站的所有网页嵌入了一个脚本，而这一注入并没有经过网站管理员的同意。最初，GoDaddy是为了改善性能的而植入名为Real User Metrics的脚本去收集用户数据，声称绝大部分用户不会感觉到问题，但脚本本身却存在导致网站加载缓慢或破坏网页的可能。
  - 链接：https://www.igorkromin.net/index.php/2019/01/13/godaddy-is-sneakily-injecting-javascript-into-your-website-and-how-to-stop-it/

- 标题：新的侧通道攻击从Windows，Linux页面缓存窃取数据
  - 时间：2019-01-08
  - 简介：近日有研究人员发现一种新的边信道攻击，利用操作系统的页面缓存窃取项目二进制文件、库、文件等敏感信息。根据研究人员的演示，Windows 和 Linux 都会受到该攻击影响，macOS 也可能受到相同影响。这个攻击不受硬件设施的限制，主要在本地发起攻击，绕过沙箱、改正定时的用户界面，而且可以恢复自动生成的临时密码。此外，远程攻击也有可能实现，不过会有条件限制。
  - 链接：https://www.bleepingcomputer.com/news/security/new-side-channel-attack-steals-data-from-windows-linux-page-cache/

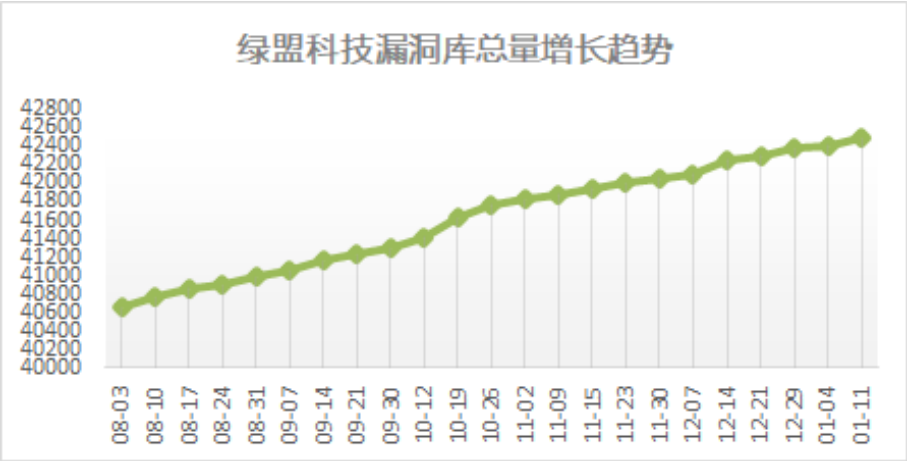
- 标题：未受保护的MongoDB暴露超过2亿份简历
  - 时间：2019-01-10
  - 简介：一个庞大的MongoDB数据库包含2亿多条记录，其中包含来自中国求职者的简历，无需认证即可访问至少一周内的求职者。缓存的大小约854GB。以这种方式曝光的信息，共计202,730,434条记录，包括人们希望在简历中看到的所有细节：个人信息（全名，出生日期，电话号码，电子邮件地址，公民身份），专业经验和工作期望。这类信息是网络犯罪分子的金矿，可以利用它来提高网络钓鱼活动的成功率。
  - 链接：https://www.bleepingcomputer.com/news/security/unprotected-mongodb-exposes-over-200-millions-resumes/

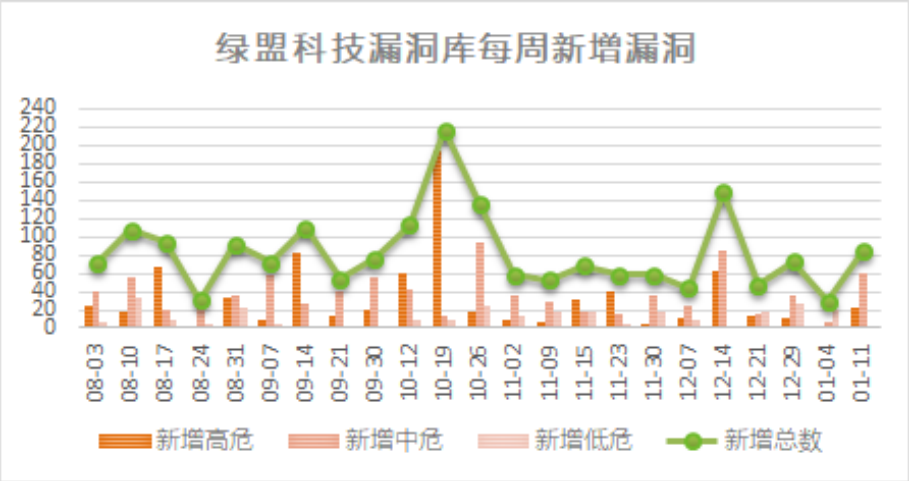
（数据来源：绿盟科技 威胁情报中心 收集整理）

# 二. 漏洞研究

## 2.1 漏洞库统计

截止到2019年01月11日，绿盟科技漏洞库已收录总条目达到42493条。本周新增漏洞记录84条，其中高危漏洞数量23条，中危漏洞数量60条，低危漏洞数量1条。




- IBM API Connect 权限提升漏洞（CVE-2018-1859）
    - 危险等级:中
    - cve编号:CVE-2018-1888
- IBM i Access for Windows 任意代码执行漏洞（CVE-2018-1888）
    - 危险等级:中
    - cve编号:CVE-2018-3956
- Foxit Reader和PhantomPDF for Windows 缓冲区溢出漏洞（CVE-2018-3956）
    - 危险等级:中
    - cve编号:CVE-2018-18688
- Foxit Reader和PhantomPDF for Windows 安全限制绕过漏洞（CVE-2018-18688）
    - 危险等级:中
    - cve编号:CVE-2019-5005
- Foxit Reader和PhantomPDF for Windows拒绝服务漏洞（CVE-2019-5005）
    - 危险等级:中
    - cve编号:CVE-2019-5006
- Foxit Reader和PhantomPDF for Windows空指针间接引用漏洞（CVE-2019-5006）
    - 危险等级:中
    - cve编号:CVE-2019-5007
- Foxit Reader和PhantomPDF for Windows 缓冲区溢出漏洞（CVE-2019-5007）
    - 危险等级:中
    - cve编号:CVE-2018-18689
- Foxit Reader和PhantomPDF for Windows 安全限制绕过漏洞（CVE-2018-18689）

    - 危险等级:中
    - cve编号:CVE-2018-4035
- MacPaw CleanMyMac X truncateFileAtPath权限提升漏洞（CVE-2018-4035）
    - 危险等级:高
    - cve编号:CVE-2018-4032
- MacPaw CleanMyMac X moveItemAtPath权限提升漏洞（CVE-2018-4032）
    - 危险等级:高
    - cve编号:CVE-2018-4034
- MacPaw CleanMyMac X removeItemAtPath权限提升漏洞（CVE-2018-4034）
    - 危险等级:高
    - cve编号:CVE-2018-4044
- MacPaw CleanMyMac X removePackageWithID 权限提升漏洞（CVE-2018-4044）
    - 危险等级:高
    - cve编号:CVE-2018-4041
- MacPaw CleanMyMac X enableLaunchdAgentAtPath权限提升漏洞（CVE-2018-4041）
    - 危险等级:高
    - cve编号:CVE-2018-4046
- MacPaw CleanMyMac X pleaseTerminate拒绝服务漏洞（CVE-2018-4046）
    - 危险等级:高
    - cve编号:CVE-2018-4042
- MacPaw CleanMyMac X removeLaunchdAgentAtPath权限提升漏洞（CVE-2018-4042）
    - 危险等级:高
    - cve编号:CVE-2018-4047
- MacPaw CleanMyMac X disableLaunchdAgentAtPath权限提升漏洞（CVE-2018-4047）
    - 危险等级:高
    - cve编号:CVE-2018-4043
- MacPaw CleanMyMac X removeASL权限提升漏洞（CVE-2018-4043）
    - 危险等级:高
    - cve编号:CVE-2018-4045
- MacPaw CleanMyMac X securelyRemoveItemAtPath权限提升漏洞（CVE-2018-4045）
    - 危险等级:高
    - cve编号:CVE-2018-4037
- MacPaw CleanMyMac X 权限提升漏洞（CVE-2018-4037）
    - 危险等级:高
    - cve编号:CVE-2018-4033
- MacPaw CleanMyMac X moveToTrashItemAtPath权限提升漏洞（CVE-2018-4033）
    - 危险等级:高
    - cve编号:CVE-2018-4036
- MacPaw CleanMyMac X removeKextAtPath权限提升漏洞（CVE-2018-4036）
    - 危险等级:高
    - cve编号:CVE-2019-3701
- Linux Kernel 'can_can_gw_rcv in net/can/gw.c' 本地拒绝服务漏洞（CVE-2019-3701）
    - 危险等级:低

    - BID:106443
    - cve编号:CVE-2019-0550
- Microsoft Windows Hyper-V远程代码执行漏洞（CVE-2019-0550）
    - 危险等级:高
    - BID:106385
    - cve编号:CVE-2019-0551
- Microsoft Windows Hyper-V远程代码执行漏洞（CVE-2019-0551）
    - 危险等级:高
    - BID:106386
    - cve编号:CVE-2019-0556
- Microsoft Office SharePoint跨站脚本漏洞（CVE-2019-0556）
    - 危险等级:中
    - BID:106387
    - cve编号:CVE-2019-0557
- Microsoft Office SharePoint跨站脚本漏洞（CVE-2019-0557）
    - 危险等级:中
    - BID:106388
    - cve编号:CVE-2019-0558
- Microsoft Office SharePoint跨站脚本漏洞（CVE-2019-0558）
    - 危险等级:中
    - BID:106389
    - cve编号:CVE-2019-0585
- Microsoft Word任意代码执行漏洞（CVE-2019-0585）
    - 危险等级:中
    - BID:106392
    - cve编号:CVE-2019-0537
- Microsoft Visual Studio信息泄露漏洞（CVE-2019-0537）
    - 危险等级:中
    - BID:106390
    - cve编号:CVE-2019-0546
- Microsoft Visual Studio任意代码执行漏洞（CVE-2019-0546）
    - 危险等级:中
    - BID:106391
    - cve编号:CVE-2019-0559
- Microsoft Outlook信息泄露漏洞（CVE-2019-0559）
    - 危险等级:中
    - BID:106397
    - cve编号:CVE-2019-0555
- Microsoft Windows 本地权限提升漏洞（CVE-2019-0555）
    - 危险等级:中
    - BID:106395
    - cve编号:CVE-2019-0547
- Microsoft Windows DHCP Client 远程代码执行漏洞（CVE-2019-0547）

    - 危险等级:高
    - BID:106394
    - cve编号:CVE-2019-0562
- Microsoft SharePoint Server远程权限提升漏洞（CVE-2019-0562）
    - 危险等级:中
    - BID:106400
    - cve编号:CVE-2019-0560
- Microsoft Office 信息泄露漏洞（CVE-2019-0560）
    - 危险等级:中
    - BID:106398
    - cve编号:CVE-2019-0561
- Microsoft Word 信息泄露漏洞（CVE-2019-0561）
    - 危险等级:中
    - BID:106399
    - cve编号:CVE-2019-0575
- Microsoft Windows JET Database Engine 远程代码执行漏洞（CVE-2019-0575）
    - 危险等级:中
    - BID:106404
    - cve编号:CVE-2019-0541
- Microsoft Internet Explorer 远程代码执行漏洞（CVE-2019-0541）
    - 危险等级:中
    - BID:106402
    - cve编号:CVE-2019-0539
- Microsoft Chakra脚本引擎远程内存破坏漏洞（CVE-2019-0539）
    - 危险等级:高
    - BID:106401
    - cve编号:CVE-2018-12817
- Adobe Digital Editions 越界读信息泄露漏洞（CVE-2018-12817）
    - 危险等级:中
    - BID:106472
    - cve编号:CVE-2018-19718
- Adobe Connect信息泄露漏洞（CVE-2018-19718）
    - 危险等级:高
    - BID:106469
    - cve编号:CVE-2019-0567
- Microsoft Edge Chakra脚本引擎远程内存破坏漏洞（CVE-2019-0567）
    - 危险等级:高
    - BID:106418
    - cve编号:CVE-2019-0566
- Microsoft Edge远程权限提升漏洞（CVE-2019-0566）
    - 危险等级:中
    - BID:106417
    - cve编号:CVE-2019-0565

- Microsoft Edge远程内存破坏漏洞（CVE-2019-0565）
    - 危险等级:高
    - BID:106416
    - cve编号:CVE-2019-0569
- Microsoft Windows Kernel本地信息泄露漏洞（CVE-2019-0569）
    - 危险等级:中
    - BID:106414
    - cve编号:CVE-2019-0570
- Microsoft Windows Runtime 本地权限提升漏洞（CVE-2019-0570）
    - 危险等级:中
    - BID:106415
    - cve编号:CVE-2019-0553
- Microsoft Windows Subsystem for Linux本地信息泄露漏洞（CVE-2019-0553）
    - 危险等级:中
    - BID:106412
    - cve编号:CVE-2019-0564
- Microsoft ASP.NET Core 拒绝服务漏洞（CVE-2019-0564）
    - 危险等级:中
    - BID:106413
    - cve编号:CVE-2019-0548
- Microsoft ASP.NET Core 拒绝服务漏洞（CVE-2019-0548）
    - 危险等级:中
    - BID:106410
    - cve编号:CVE-2019-0554
- Microsoft Windows Kernel本地信息泄露漏洞（CVE-2019-0554）
    - 危险等级:中
    - BID:106411
    - cve编号:CVE-2019-0549
- Microsoft Windows Kernel本地信息泄露漏洞（CVE-2019-0549）
    - 危险等级:中
    - BID:106409
    - cve编号:CVE-2019-0536
- Microsoft Windows Kernel本地信息泄露漏洞（CVE-2019-0536）
    - 危险等级:中
    - BID:106406
    - cve编号:CVE-2019-0552
- Microsoft Windows COM本地权限提升漏洞（CVE-2019-0552）
    - 危险等级:中
    - BID:106407
    - cve编号:CVE-2019-0543
- Microsoft Windows 本地权限提升漏洞（CVE-2019-0543）
    - 危险等级:中

    - BID:106408
    - cve编号:CVE-2019-0545
- Microsoft ASP.NET Core 信息泄露漏洞（CVE-2019-0545）
    - 危险等级:中
    - BID:106405
    - cve编号:CVE-2019-0538
- Microsoft Windows JET Database Engine 远程代码执行漏洞（CVE-2019-0538）
    - 危险等级:中
    - BID:106419
    - cve编号:CVE-2019-0568
- Microsoft Edge Chakra脚本引擎远程内存破坏漏洞（CVE-2019-0568）
    - 危险等级:高
    - BID:106420
    - cve编号:CVE-2019-0586
- Microsoft Exchange 远程内存破坏漏洞（CVE-2019-0586）
    - 危险等级:中
    - BID:106421
    - cve编号:CVE-2019-0576
- Microsoft Windows JET Database Engine 远程代码执行漏洞（CVE-2019-0576）
    - 危险等级:中
    - BID:106422
    - cve编号:CVE-2019-0577
- Microsoft Windows JET Database Engine 远程代码执行漏洞（CVE-2019-0577）
    - 危险等级:中
    - BID:106423
    - cve编号:CVE-2019-0578
- Microsoft Windows JET Database Engine 远程代码执行漏洞（CVE-2019-0578）
    - 危险等级:中
    - BID:106424
    - cve编号:CVE-2019-0579
- Microsoft Windows JET Database Engine 远程代码执行漏洞（CVE-2019-0579）
    - 危险等级:中
    - BID:106425
    - cve编号:CVE-2019-0571
- Microsoft Windows Data Sharing Service 本地权限提升漏洞（CVE-2019-0571）
    - 危险等级:中
    - BID:106426
    - cve编号:CVE-2019-0572
- Microsoft Windows Data Sharing Service 本地权限提升漏洞（CVE-2019-0572）
    - 危险等级:中
    - BID:106428
    - cve编号:CVE-2019-0580
- Microsoft Windows JET Database Engine 远程代码执行漏洞（CVE-2019-0580）

    - 危险等级:中
    - BID:106429
    - cve编号:CVE-2019-0573
- Microsoft Windows Data Sharing Service 本地权限提升漏洞（CVE-2019-0573）
    - 危险等级:中
    - BID:106430
    - cve编号:CVE-2019-0574
- Microsoft Windows Data Sharing Service 本地权限提升漏洞（CVE-2019-0574）
    - 危险等级:中
    - BID:106431
    - cve编号:CVE-2019-0581
- Microsoft Windows JET Database Engine 远程代码执行漏洞（CVE-2019-0581）
    - 危险等级:中
    - BID:106432
    - cve编号:CVE-2019-0582
- Microsoft Windows JET Database Engine 远程代码执行漏洞（CVE-2019-0582）
    - 危险等级:中
    - BID:106433
    - cve编号:CVE-2019-0583
- Microsoft Windows JET Database Engine 远程代码执行漏洞（CVE-2019-0583）
    - 危险等级:中
    - BID:106435
    - cve编号:CVE-2019-0584
- Microsoft Windows JET Database Engine 远程代码执行漏洞（CVE-2019-0584）
    - 危险等级:中
    - BID:106436
    - cve编号:CVE-2019-0588
- Microsoft Exchange Server远程信息泄露漏洞（CVE-2019-0588）
    - 危险等级:中
    - BID:106437
    - cve编号:CVE-2019-0622
- Microsoft Skype for Android 本地权限提升漏洞（CVE-2019-0622）
    - 危险等级:中
    - BID:106465
    - cve编号:CVE-2018-15457
- Cisco Prime Infrastructure 信息泄露安全漏洞（CVE-2018-15457）
    - 危险等级:中
    - cve编号:CVE-2018-15464
- Cisco ASR 900 Series ASR拒绝服务漏洞（CVE-2018-15464）
    - 危险等级:中
    - cve编号:CVE-2018-15466
- Cisco Policy Suite Graphite只读访问安全漏洞（CVE-2018-15466）
    - 危险等级:中

        - cve编号:CVE-2018-15453
- Cisco Email Security Appliance 拒绝服务漏洞（CVE-2018-15453）
        - 危险等级:高
        - cve编号:CVE-2018-0461
- Cisco IP Phone 8800 Series 任意脚本注入漏洞（CVE-2018-0461）
        - 危险等级:中
        - cve编号:CVE-2018-15460
- Cisco Email Security Appliance 拒绝服务漏洞（CVE-2018-15460）
        - 危险等级:高
        - cve编号:CVE-2018-0474
- Cisco Unified Communications Manager信息泄露安全漏洞（CVE-2018-0474）
        - 危险等级:中
        - cve编号:CVE-2018-15458
- Cisco Firepower Management Center拒绝服务漏洞（CVE-2018-15458）
        - 危险等级:中
        - cve编号:CVE-2018-15463
- Cisco Identity Services Engine 跨站脚本安全漏洞（CVE-2018-15463）
        - 危险等级:中
        - cve编号:CVE-2018-15440
- Cisco Identity Services Engine 跨站脚本安全漏洞（CVE-2018-15440）
        - 危险等级:中
        - cve编号:CVE-2018-15456
- Cisco Identity Services Engine 密码恢复安全漏洞（CVE-2018-15456）
        - 危险等级:中
        - cve编号:CVE-2018-15456

（数据来源：绿盟威胁情报中心）

## 2.2 焦点漏洞

- 焦点漏洞
        - Microsoft Word任意代码执行漏洞
        - CVE ID
                - CVE-2019-0585
        - NSFOCUS ID
                - 42437
        - 受影响版本
                - Microsoft Office 2019
                - Microsoft Office 2016
                - Microsoft Office 2010
                - Microsoft Word 2016
                - Microsoft Word 2013
                - Microsoft Word 2010
                - Microsoft SharePoint Server 2019

        - Microsoft SharePoint Enterprise Server 2016
        - Microsoft SharePoint Enterprise Server 2013 SP1
    - 漏洞点评
        - Microsoft Office是微软公司开发的一套基于Windows操作系统的办公软件套装。Microsoft Word在内存对象的处理方式中存在远程代码执行漏洞。远程攻击者可借助特制的文件，利用该漏洞在当前用户安全上下文中执行操作。目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的页面下载。 （数据来源：绿盟威胁情报中心） （数据来源：绿盟威胁情报中心）