绿盟科技互联网安全威胁周报

——第201522期

NSFOCUS

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基本持平。公告数量排名前五的厂商/项目为IBM(16),wireshark(9),linux(8),HP(6),arubanetworks(6):。值得关注的高危漏洞如下：

CVE编号	CVSS评分	厂商
CVE-2015-2110	10	hp
CVE-2015-3331	9.3	linux
CVE-2015-1550	9	arubanetworks
CVE-2015-2123	9	hp
CVE-2015-0160	9	ibm

CVE-2014-6628	9	arubanetworks
CVE-2015-2120	8.7	hp
CVE-2015-3810	7.8	wireshark
CVE-2015-2122	7.8	hp
CVE-2015-2121	7.8	hp
CVE-2015-1157	7.8	apple
CVE-2015-3812	7.8	wireshark
CVE-2015-3809	7.8	wireshark
CVE-2015-3808	7.8	wireshark
CVE-2014-8147	7.5	icu_project
CVE-2015-0120	7.5	ibm
CVE-2015-0935	7.5	bomgar
CVE-2015-0986	7.5	moxa
CVE-2015-2945	7.5	h-fj
CVE-2014-8146	7.5	icu_project

1.2 威胁信息回顾

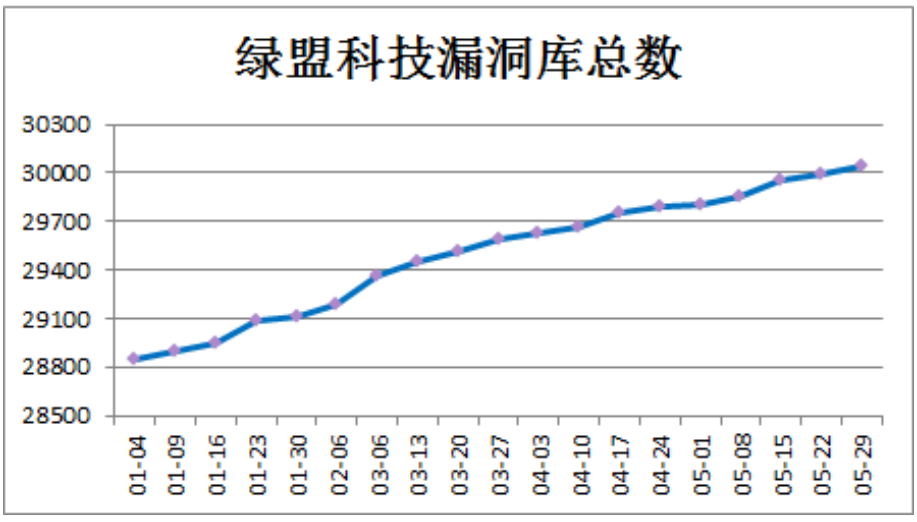
日期	信息
2015/05/25	PHP PHAR 'phar_tar_process_metadata()' Function Heap Memory Corruption Vulnerability 来源：http://www.securityfocus.com/bid/74703 简述：攻击者利用这个问题，可以在受影响应用程序上下文中执行任意代码。 CVE-编号：2015-3307
2015/05/26	万达电商某站漏洞影响4600万会员数据 来源：http://www.wooyun.org/bugs/wooyun-2015-0115981 简述：万达电商某站漏洞影响4600万会员数据
2015/05/26	南阳市公安局交通管理支队存在sql注入漏洞可导致泄露大量信息 来源：http://www.wooyun.org/bugs/wooyun-2015-0115963 简述：南阳市公安局交通管理支队存在sql注入漏洞可导致泄露大量信息
2015/05/26	一曲田商城存在注入可获取500w+用户信息和600w+商户信息 来源：http://www.wooyun.org/bugs/wooyun-2015-0116138 简述：一曲田商城存在注入可获取500w+用户信息和600w+商户信息

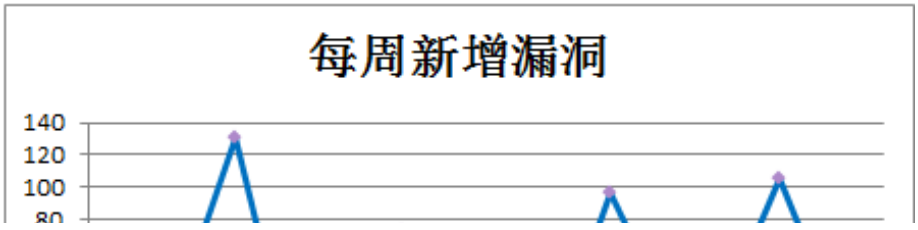
（数据来源：绿盟科技 威胁响应中心 收集整理）

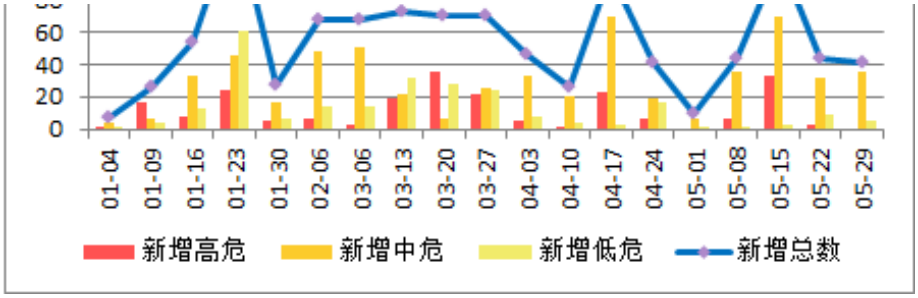
二. 漏洞研究

2.1 漏洞库统计

截止到2015年5月29日，绿盟科技漏洞库已收录总条目达到30038条。本周新增漏洞记录41条，其中高危漏洞数量0条，中危漏洞数量36条，低危漏洞数量5条。







NSF-ID	漏洞名称	危险等级	BID	CVE编号
29998	PostgreSQL信息泄露漏洞(CVE-2015-3166)	中	74790	CVE-2015-3166
29999	WordPress Simple Photo Gallery插件'index.php' SQL注入漏洞	中	74784	
30000	WordPress Landing Pages插件SQL注入及跨站脚本漏洞	中	74777	
30001	PostgreSQL远程拒绝服务漏洞(CVE-2015-3165)	中	74787	CVE-2015-3165
30002	HP SiteScope远程权限提升漏洞(CVE-2015-2120)	中		CVE-2015-2120
30003	Apache Hive身份验证漏洞(CVE-2015-1772)	中		CVE-2015-1772
30004	Cisco TelePresence TC/TE软件身份验证绕过漏洞(CVE-2014-2174)	中	74639	CVE-2014-2174
30005	Cisco TelePresence TC/TE软件拒绝服务漏洞(CVE-2015-0722)	中	74636	CVE-2015-0722
30006	Cisco Access Control Server远程拒绝服务漏洞(CVE-2015-0746)	中	74771	CVE-2015-0746
30007	MIT Kerberos 5 requires_preauth绕过漏洞(CVE-2015-2694)	中		CVE-2015-2694
30008	QEMU 'net/slirp.c'不安全临时文件创建漏洞	中	74809	CVE-2015-4037
30009	Apache Ambari '/var/lib/ambari-server/ambari-env.sh'本地权限提升漏洞	中	74686	
30010	GNU Coreutils 'src/sort.c'多个缓冲区溢出漏洞	中	74688	
30011	Cisco Unified Customer Voice Portal跨站请求伪造漏洞(CVE-2015-0735)	中	73697	CVE-2015-0735
30012	Cisco Unified Communications Manager多个安全漏洞(CVE-2015-0749)	中	74785	CVE-2015-0749
30013	Emerson AMS Device Manager本地SQL注入漏洞(CVE-2015-1008)	中	74774	CVE-2015-1008
30014	Apache HBase多个远程漏洞(CVE-2015-1836)	中		CVE-2015-1836
30015	Apache Jackrabbit XML外部实体信息泄露漏洞(CVE-2015-1833)	低	74761	CVE-2015-1833
30016	Linux Kernel "vhost_scsi_make_tpg()"内存破坏漏洞(CVE-2015-4036)	中		CVE-2015-4036
30017	Schneider Electric OPC Factory Server DLL加载任意代码执行漏洞	中	74772	CVE-2015-1014
30018	python-kerberos 'checkPassword()'函数中间人信息泄露漏洞	低	74760	CVE-2015-3206
30019	Dell NetVault Backup堆缓冲区溢出远程代码执行漏洞	中		CVE-2015-4067
30020	Cisco Adaptive Security Appliance拒绝服务漏洞(CVE-2015-0742)	中	74750	CVE-2015-0742

30021	Linux kernel Btrfs权限提升漏洞(CVE-2014-9710)	中		CVE-2014-9710
30022	Sourcefire Defense Center/3D Sensor任意文件上传漏洞	低		CVE-2015-0739
30023	Linux Kernel本地权限提升漏洞(CVE-2015-3339)	低	74243	CVE-2015-3339
30024	Cisco IP Phone 7861拒绝服务漏洞(CVE-2015-0751)	中		CVE-2015-0751
30025	osCmax多个跨站请求伪造漏洞(CVE-2012-6691)	中	74753	CVE-2012-6691
30026	Cisco Prime Central for HCS多个跨站请求伪造漏洞(CVE-2015-0741)	中	74754	CVE-2015-0741
30027	多个IBM产品拒绝服务漏洞(CVE-2014-8926)	中	74780	CVE-2014-8926
30028	多个IBM产品拒绝服务漏洞(CVE-2014-8927)	中	74779	CVE-2014-8927
30029	Apache Cordova Android远程利用辅助配置变量漏洞(CVE-2015-1835)	中		CVE-2015-1835
30030	Cisco Wireless LAN Controller TCP流量处理拒绝服务漏洞	低		CVE-2015-0756
30031	phpwind goto.php开放重定向漏洞(CVE-2015-4134)	中		CVE-2015-4134
30032	phpwind goto.php跨站脚本漏洞(CVE-2015-4135)	中		CVE-2015-4135
30033	Aruba Networks CPPM 跨站脚本漏洞(CVE-2015-4132)	中		CVE-2015-4132
30034	Aruba Networks CPPM目录遍历漏洞(CVE-2015-1551)	中		CVE-2015-1551
30035	Aruba Networks CPPM目录遍历漏洞(CVE-2015-1550)	中		CVE-2015-1550
30036	Aruba Networks CPPM SQL注入漏洞(CVE-2015-1392)	中		CVE-2015-1392
30037	Aruba Networks CPPM 跨站脚本漏洞(CVE-2015-1389)	中		CVE-2015-1389
30038	Aruba Networks CPPM远程代码执行漏洞(CVE-2014-6628)	中		CVE-2014-6628

（数据来源：绿盟科技安全研究部&产品规则组）

2.2 焦点漏洞

漏洞描述	**Microsoft Windows 本地权限提升漏洞(CVE-2015-1701)(MS15-051)**
NSFOCUS ID	**29906**
Bugtraq ID	**74245**
CVE ID	**CVE-2015-1701**
漏洞点评	Win32k.sys内核模式驱动程序没有正确处理内存对象，在实现上存在权限提升漏洞，成功利用此漏洞可使攻击者在内核模式中运行任意代码。目前已经出现利用工具，可能导致大范围的对此漏洞的利用攻击。强烈建议用户检查自己的系统是否为最新版本，如不是，尽快升级。

（数据来源：绿盟科技安全研究部&产品规则组）