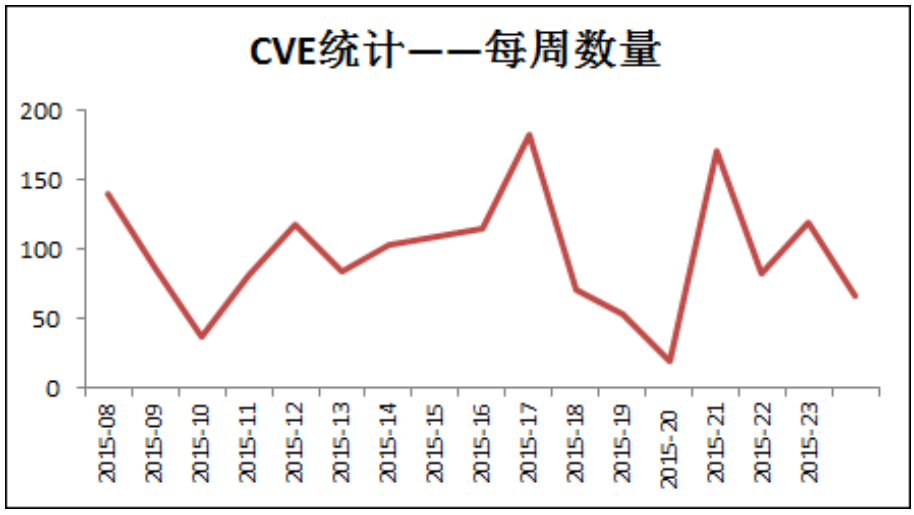
绿盟科技互联网安全威胁周报

——第201523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有所下降。公告数量排名前五的厂商/项目为moodle(25)、cisco(8)、sap(7)、apache(3)、xen(3):。值得关注的高危漏洞如下:

CVE编号	CVSS评分	厂商
CVE-2015-0850	10	fusionforge
CVE-2015-4104	7.8	xen
CVE-2015-4159	7.5	sap
CVE-2015-2282	7.5	sap
CVE-2015-4161	7.5	sap
CVE-2015-4160	7.5	sap
CVE-2015-4106	7.2	qemu
CVE-2015-0761	7.2	cisco
CVE-2015-2268	6.8	moodle
CVE-2015-0217	6.8	moodle
CVE-2015-2124	6.8	hp
CVE-2015-0541	6.8	emc
CVE-2015-1000	6.8	moxa
CVE-2015-0759	6.8	cisco
CVE-2015-0213	6.8	moodle
CVE-2015-0218	6.8	moodle
CVE-2015-3950	6.8	xzeres
CVE-2015-1493	6.8	moodle
CVE-2015-1945	6.5	ibm
CVE-2015-4038	6.5	wpmembership

1.2 威胁信息回顾

日期	信息
2015/06/01	行动代号OpChina：国际黑客组织匿名者（Anonymous）宣布今日发动对华网络攻击 来源：http://www.freebuf.com/news/68672.html 简述：国际黑客组织匿名者（Anonymous）联合计划于2015年5月30日发动对华网络攻击，行动代号”OpChina”。目前日本、菲律宾、越南的黑客已响应行动。由于事件的升级，黑客大战已于29日悄悄提前开始了。
2015/06/02	风讯CMS存在SQL注入漏洞 来源：http://www.wooyun.org/bugs/wooyun-2015-0117395 简述：风讯CMS存在SQL注入漏洞
2015/06/03	社会管理综合治理信息系统弱口令泄露公民信息等（涉及浙江、山东） 来源：http://www.wooyun.org/bugs/wooyun-2015-0117791 简述：社会管理综合治理信息系统弱口令泄露公民信息等（涉及浙江、山东）
2015/06/04	中国电信企业应用可重置任意用户密码漏洞（泄露用户大量订单信息\域名\邮箱\云盘\建站信息） 来源：http://www.wooyun.org/bugs/wooyun-2015-0118020 简述： 中国电信企业应用可重置任意用户密码漏洞（泄露用户大量订单信息\域名\邮箱\云

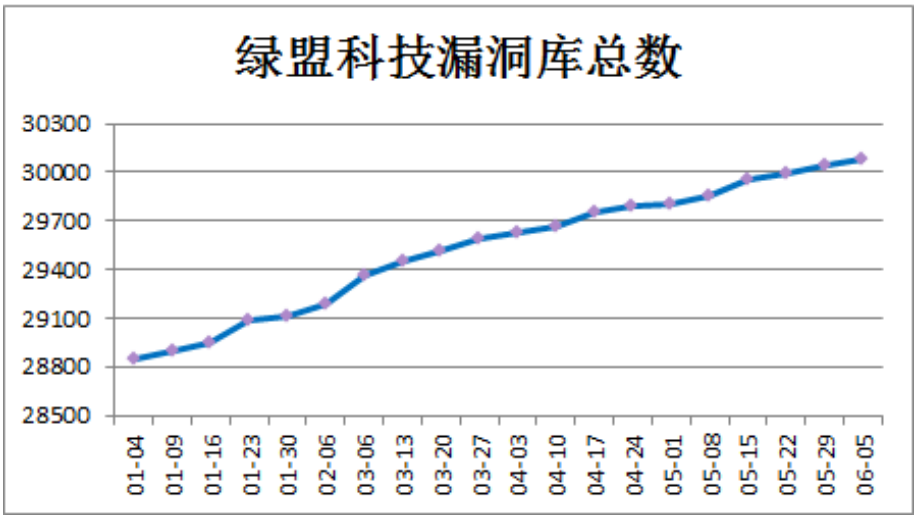
盘\建站信息）

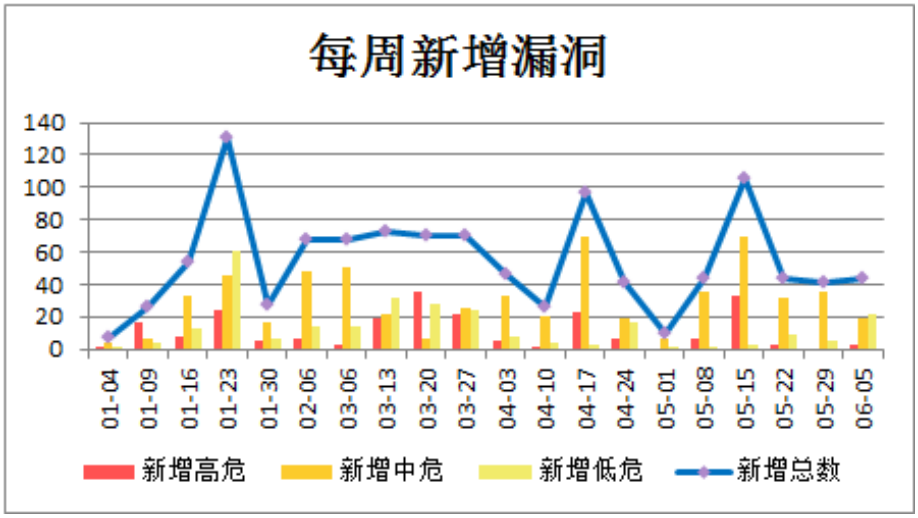
（数据来源：绿盟科技 威胁响应中心 收集整理）

二. 漏洞研究

2.1 漏洞库统计

截止到2015年6月5日，绿盟科技漏洞库已收录总条目达到30081条。本周新增漏洞记录43条，其中高危漏洞数量3条，中危漏洞数量19条，低危漏洞数量21条。





NSF-ID	漏洞名称	危险等级	BID	CVE编号
30039	Rockwell Automation RSView32信息泄露漏洞(CVE-2015-1010)	低		CVE-2015-1010
30040	PHP空字符不完整修复多个安全功能绕过漏洞(CVE-2015-4025)	低	74904	CVE-2015-4025
30041	多个IBM产品本地权限提升漏洞(CVE-2015-0121)	低	74910	CVE-2015-0121
30042	Linux Kernel 'fs_pin.c'空指针间接引用拒绝服务漏洞	低	74915	
30043	IBM PowerVC身份验证绕过漏洞(CVE-2015-1937)	中	74911	CVE-2015-1937
30044	多个D-Link产品缓冲区溢出漏洞(CVE-2014-7859)	中	74878	CVE-2014-7859
	D-Link DIR-645路由器远程任意命令执行漏洞(CVE-2015-			

30045	2051)	中	74870	CVE-2015-2051
30046	Google Chrome安全限制绕过漏洞(CVE-2015-2239)	中	74855	CVE-2015-2239
30047	WordPress Survey and Poll插件'settings.php' SQL注入漏洞	低	74890	CVE-2015-2090
30048	WordPress Video Gallery 插件'videogalleryrss.php' SQL注入漏洞	中	74882	CVE-2015-2065
30049	WordPress Photocrati主题'ecomm-sizes.php' SQL注入漏洞	中	74854	CVE-2015-2216
30050	WordPress Estrutura-Basica主题'download.php'任意文件下载漏洞	中	74828	
30051	Linux Kernel 'tty/tty_ldsem.c'本地竞争条件漏洞	低	74820	
30052	PHP 'main/rfc1867.c'远程拒绝服务漏洞	中	74903	CVE-2015-4024
30053	PHP 'ftp_genlist()'函数整数溢出漏洞	中	74902	CVE-2015-4022
30054	Wireshark Android Logcat文件解析器 'wiretap/logcat.c'拒绝服务漏洞	中	74837	CVE-2015-3906
30055	HP HP-Plugin远程代码执行漏洞(CVE-2015-0839)	中	74913	CVE-2015-0839
30056	SAP Afaria信息泄露漏洞(CVE-2015-4161)	低		CVE-2015-4161
30057	Apache Sling API多个跨站脚本漏洞(CVE-2015-2944)	高		CVE-2015-2944
30058	GNU Parallel任意文件写漏洞(CVE-2015-4155)	中		CVE-2015-4155
30059	GNU Parallel任意文件写漏洞(CVE-2015-4156)	中		CVE-2015-4156
30060	SAP Content Server拒绝服务漏洞(CVE-2015-4157)	低		CVE-2015-4157
30061	SAP ABAP & Java Server拒绝服务漏洞(CVE-2015-4158)	低		CVE-2015-4158
30062	SAP HANA SQL注入漏洞(CVE-2015-4159)	低		CVE-2015-4159
30063	SAP ASE Database Platform SQL注入漏洞(CVE-2015-4160)	低		CVE-2015-4160
30064	Apple Mac电脑固件0day EFI rootkit漏洞	高		
30065	RSA Web Threat Detection跨站请求伪造漏洞(CVE-2015-0541)	低		CVE-2015-0541
30066	QEMU未调解的PCI寄存器访问漏洞(CVE-2015-4106)	低		CVE-2015-4106
30067	Apache Camel信息泄露漏洞(CVE-2015-0263)	低		CVE-2015-0263
30068	Apache Camel信息泄露漏洞(CVE-2015-0264)	低		CVE-2015-0264
30069	Xen拒绝服务漏洞(CVE-2015-4103)	低		CVE-2015-4103
30070	Xen拒绝服务漏洞(CVE-2015-4104)	低		CVE-2015-4104
30071	Xen拒绝服务漏洞(CVE-2015-4105)	低		CVE-2015-4105
30072	Cisco AnyConnect Secure Mobility Client权限提升漏洞(CVE-2015-0761)	中		CVE-2015-0761

30073	多个思科产品拒绝服务漏洞(CVE-2015-0744)	低	74916	CVE-2015-0744
30074	Linux Kernel 'fs/pipe.c'多个本地内存破坏漏洞(CVE-2015-1805)	中	74951	CVE-2015-1805
30075	Cisco Adaptive Security Appliance XAUTH安全功能绕过漏洞(CVE-2015-0760)	中	74957	CVE-2015-0760
30076	Cisco Unified MeetingPlace信息泄露漏洞(CVE-2015-0763)	中	74955	CVE-2015-0763
30077	Adobe Flash Player SWF文件处理本地信息泄露漏洞	低	74925	
30078	Django 'session.flush()'函数会话固定漏洞(CVE-2015-3982)	低	74960	CVE-2015-3982
30079	腾讯微信客户端拒绝服务漏洞	高		
30080	Cisco FireSIGHT System Software跨站脚本及HTML注入漏洞(CVE-2015-0766)	中	75003	CVE-2015-0766
30081	Cisco ONS 15454 System Software拒绝服务漏洞(CVE-2015-0765)	中	75002	CVE-2015-0765

（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	**Adobe Flash Player内存破坏漏洞(CVE-2015-3043)**
NSFOCUS ID	**29735**
Bugtraq ID	
CVE ID	**CVE-2015-3043**
漏洞点评	Adobe Flash Player在实现上存在内存破坏漏洞，攻击者利用此漏洞可执行任意代码或造成拒绝服务。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系统上的Adobe Flash Player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）