中国科学院国家天文台

综述

任务名称	扫描［中国科学院国家天文台］
网络风险	风险值:10
主机统计	已扫描主机数：70 非常危险主机：27
使用模板	自动匹配扫描
时间统计	开始：2016-03-14 13:09:47 结束：2016-03-14 14:08:29
系统版本	5.0.13.59
非	

目录

风险类别

服务分类

风.

分类名	高风险	中风险	低风险	总计
ONC/RPC	0	0	9	9
WWW	22	98	19	139
POP3	0	0	1	1
SSH	5	8	7	20
数据库	3	46	20	69
FTP	0	2	2	4
CGI	0	0	1	1
DNS	8	8	5	21
AntiVirus	0	0	2	2
远程管理	0	0	1	1
IMAP	0	0	1	1
SMTP	0	0	2	2
X Window	0	0	1	1
LDAP	0	0	1	1
Kernel	0	0	1	1
其他	0	4	3	7

系统分类

风.

分类名	高风险	中风险	低风险	总计
UNIX通用	1	3	12	16
系统无关	36	159	60	255
Windows	1	3	4	8

分类名	高风险	中风险	低风险	总计
Linux	0	1	0	1

应用程序分布

风.

分类名	高风险	中风险	低风险	总计
Apache	6	41	7	54
RPC	0	0	6	6
MS SQL Server	0	0	1	1
MySQL	3	46	18	67
BIND	8	8	5	21
Symantec	0	0	1	1
Tomcat	1	19	1	21
SSH	0	0	1	1
DB2	0	0	1	1
Terminal Server	0	0	1	1
OpenSSH	5	8	5	18
PHP	12	21	1	34
OpenLDAP	0	0	1	1
IIS	0	2	0	2
Sendmail	0	0	1	1
其他	3	21	26	50

威胁程度分布

风.

分类名	高风险	中风险	低风险	总计
不必要的服务	0	1	13	14
远程信息泄露	1	16	28	45
远程拒绝服务	9	21	7	37
本地权限提升	2	4	0	6
远程执行命令	1	3	1	5
远程数据修改	1	3	0	4
其他	24	118	27	169

时间分类

风.

分类名	高风险	中风险	低风险	总计
2000年	0	0	3	3
2010年	1	19	0	20
1999年	0	0	18	18
2001年	0	0	13	13
2003年	0	2	1	3
2007年	2	11	5	18
2012年	8	20	7	35
2009年	4	7	2	13
2005年	0	1	1	2
2006年	3	4	0	7
2015年	6	23	6	35
2008年	0	9	3	12
2011年	2	21	6	29

分类名	高风险	中风险	低风险	总计
2013年	5	9	0	14
2002年	0	0	1	1
2014年	7	40	10	57

主机风险等级列表

IP地址	主机名	操作系统	高风险	中风险	低风险	风险值
159.226.88.27		Windows	2	34	14	10
159.226.88.33		--	2	5	4	10
159.226.88.35		--	4	11	12	10
159.226.88.47		--	5	30	8	10
159.226.88.48		--	0	9	4	10
159.226.88.54		Unix/Linux	3	24	11	10
159.226.88.60		Windows 2003	1	23	15	10
159.226.88.66		Ubuntu Linux	8	50	17	10
159.226.88.76		Debian Linux	2	5	6	10
159.226.88.81		--	2	6	7	10
159.226.88.82	lss.bao.ac.cn	Ubuntu Linux	0	20	5	10
159.226.88.87		Unix/Linux	4	7	18	10
159.226.88.89		Unix/Linux	4	50	28	10
159.226.88.90	cosmology.bao.ac.cn	--	2	5	8	10
159.226.88.94		CentOS Linux	0	19	4	10
159.226.88.98		--	2	1	0	7.1
159.226.88.110		Windows	4	32	7	10
159.226.168.11		Red Hat Linux	7	40	16	10
159.226.168.12	21cma	Debian Linux	9	24	15	10
159.226.169.53		--	2	6	7	10
159.226.170.24		--	2	5	6	10
159.226.170.35		CentOS Linux	2	25	9	10
159.226.170.67		Unix/Linux	4	6	11	10

159.226.170.68		CentOS Linux	0	38	8	10
159.226.170.69		Unix/Linux	2	5	14	10
159.226.170.112		--	4	6	5	10
159.226.170.124		Unix/Linux	13	29	2	10
159.226.88.1		--	0	0	1	2.1
159.226.88.30		Windows	0	2	0	3.1
159.226.88.92	ARCGIS	Windows 2003	0	2	3	4.2
159.226.88.242		--	0	1	1	2.6
159.226.88.3		--	0	0	3	1.3
159.226.88.6		--	0	0	1	1.1
159.226.88.7		--	0	0	1	1.1
159.226.88.10		--	0	0	1	1.1
159.226.88.12		--	0	0	0	0
159.226.88.21		--	0	0	2	1.2
159.226.88.39		--	0	0	2	1.7
159.226.88.59		--	0	0	0	0
159.226.88.79		--	0	0	1	1.1
159.226.88.95		Windows	0	0	6	1.6
159.226.88.96		--	0	0	2	1.2
159.226.88.99		--	0	0	2	1.2
159.226.88.100		--	0	0	0	0
159.226.88.101		--	0	0	0	0
159.226.88.111		--	0	0	0	0
159.226.88.241		--	0	0	0	0
159.226.88.255		--	0	0	3	1.6
159.226.168.1		--	0	0	3	1.6
159.226.168.252		--	0	0	0	0
159.226.168.255		--	0	0	1	1.1
159.226.169.49		--	0	0	1	1.1
159.226.170.57		--	0	0	0	0
159.226.170.58		--	0	0	3	1.3
159.226.170.78		--	0	0	0	0
159.226.170.113		--	0	0	0	0
159.226.170.114		--	0	0	0	0
159.226.170.122		--	0	0	0	0
159.226.170.123		--	0	0	0	0

159.226.170.125	--	0	0	1	1.1
159.226.170.133	--	0	0	0	0
159.226.170.135	--	0	0	0	0
159.226.170.136	--	0	0	0	0
159.226.170.137	--	0	0	0	0
159.226.170.200	--	0	0	0	0
159.226.170.201	--	0	0	0	0
159.226.170.255	--	0	0	0	0
159.226.171.1	--	0	0	0	0
159.226.171.103	--	0	0	0	0
159.226.171.254	--	0	0	0	0

漏洞分布

漏洞名称	出现次数
OpenSSH复制块远程拒绝服务漏洞	1
PHP 'sapi/apache2handler/sapi_apache2.c'远程代码执行漏洞(CVE-2015-3330)	1
MySQL服务器RENAME TABLE系统表格覆盖漏洞	1
Apache mod_deflate模块远程拒绝服务漏洞	3
MySQL sql_parse.cc远程格式串漏洞	1
ISC BIND 9 'libdns'远程拒绝服务漏洞(CVE-2013-2266)	3
ISC BIND 9 DNS64 REQUIRE断言失败拒绝服务漏洞	1
OpenSSH J-PAKE授权问题漏洞(CVE-2010-4478)	14
ISC BIND 9 DNS资源记录处理远程拒绝服务漏洞(CVE-2012-1667)	1
ISC BIND 9 DNSSEC验证远程拒绝服务漏洞	3
Apache 'mod_proxy_balancer' 模块存在未明漏洞(CVE-2007-6423)	1
OpenSSH sshd Privilege Separation Monitor 未明漏洞	5
Apache Tomcat DIGEST身份验证多个安全漏洞(CVE-2012-3439)	1
ISC BIND 9 DNS64 远程拒绝服务漏洞(CVE-2012-5689)	1
Apache mod_proxy反向代理拒绝服务漏洞	3
Apache mod_proxy_ftp模块远程命令注入漏洞	3
Apache HTTP Server畸形Range和Range-Request选项处理远程拒绝服务漏洞【原理扫描】	2
ISC BIND 9 DNS资源记录处理远程拒绝服务漏洞(CVE-2012-4244)	3
ISC BIND 9 DNS RDATA处理远程拒绝服务漏洞(CVE-2012-5166)	3
Apache HTTP Server mod_session_dbd远程安全漏洞(CVE-2013-2249)	1
ISC BIND 9 DNS RDATA处理远程拒绝服务漏洞(CVE-2013-4854)	3
phpMyAdmin多个安全漏洞(CVE-2011-2506)	1
Nginx 'access.log'不安全文件权限漏洞（CVE-2013-0337）	1
Portable OpenSSH GSSAPI远程代码执行漏洞(CVE-2006-5051)	5

漏洞名称	出现次数
nginx URI处理安全限制绕过漏洞(CVE-2013-4547)	1
PHP OpenSSL Extension 'openssl_x509_parse()'内存破坏漏洞(CVE-2013-6420)	1
OpenSSH 'schnorr.c'远程内存破坏漏洞(CVE-2014-1692)	15
Oracle MySQL Server远程安全漏洞(CVE-2015-0411)	1
PHP "Unserialize()"函数释放后重利用远程代码执行漏洞	1
PHP 'cgi_main.c'越界读拒绝服务漏洞(CVE-2014-9427)	1
PHP libmagic/apprentice.c apprentice_load函数拒绝服务漏洞(CVE-2014-9426)	1
PHP堆缓冲区溢出漏洞(CVE-2014-9705)	1
PHP ZIP扩展libzip 数字错误漏洞(CVE-2015-2331)	1
PHP‘process_nested_data’函数释放后重用漏洞(CVE-2015-2787)	1
PHP拒绝服务漏洞（CVE-2014-3669）	1
PHP FPM 'php-fpm.conf.in'本地权限提升漏洞(CVE-2014-0185)	1
PHP不完整修复释放后重利用远程代码执行漏洞(CVE-2015-0231)	1
PHP multipart/form-data 远程DOS漏洞	1
Apache mod_proxy_http模块超时处理信息泄露漏洞	7
Apache Tomcat拒绝服务漏洞(CVE-2012-2733)	1
Apache Tomcat FORM身份验证安全绕过漏洞	1
Apache HTTP Server mod_proxy_ajp模块拒绝服务漏洞	8
MySQL IF查询处理远程拒绝服务漏洞	1
MySQL SQL SECURITY INVOKER存储过程权限提升漏洞	1
MySQL连接查询拒绝服务漏洞	1
MySQL/MariaDB Server用户存在弱口令	1
MySQL访问验证及拒绝服务漏洞	1
MySQL Server权限提升及拒绝服务漏洞	1
Apache HTTP服务器403 Error页面跨站脚本漏洞	2
OpenSSH X连接会话劫持漏洞	1
Apache mod_proxy_ftp模块通配符字符跨站脚本漏洞	2
Oracle MySQL 任意SQL命令执行漏洞(CVE-2009-5026)	1
Apache mod_negotiation模块HTML注入及HTTP响应拆分漏洞	2
Apache Tomcat 跨站请求伪造漏洞	1
Apache Tomcat HTTP Digest Access Authentication 安全绕过漏洞(CVE-2012-5886)	1
Apache Tomcat HTTP Digest Access Authentication实现安全漏洞(CVE-2012-5887)	1
Apache HTTP Server多个模块主机名和URI跨站脚本漏洞(CVE-2012-3499)	14
MySQL OpenSSL客户端绕过yaSSL服务器证书验证漏洞	1

漏洞名称	出现次数
MySQL CREATE TABLE调用绕过访问限制漏洞	1
phpMyAdmin输入验证漏洞(CVE-2011-0986)	1
MySQL错误UNINSTALL PLUGIN权限检查漏洞	1
MySQL COM_FIELD_LIST命令远程溢出漏洞	1
MySQL COM_FIELD_LIST命令绕过权限检查漏洞	1
Apache Tomcat replay-countermeasure功能安全漏洞	1
phpMyAdmin跨站脚本漏洞(CVE-2011-1940)	1
phpMyAdmin输入验证漏洞(CVE-2011-2719)	1
Apache CGI脚本源码信息泄露漏洞(CVE-2006-4110)	1
Apache HTTP Server balancer_handler函数跨站脚本漏洞	14
OpenSSH默认服务器配置拒绝服务漏洞(CVE-2010-5107)	16
ISC BIND UPDATE请求处理拒绝服务漏洞	2
thc ssl dos攻击【原理扫描】	1
Oracle MySQL Server远程拒绝服务漏洞(CVE-2012-0490)	1
Oracle MySQL Server远程信息泄露漏洞(CVE-2012-0484)	1
Apache HTTP Server “ap_pregsub()”函数本地权限提升漏洞	11
Apache HTTP Server mod_proxy_ajp拒绝服务漏洞	11
Oracle MySQL Server远程拒绝服务漏洞(CVE-2012-0101)	1
Apache HTTP Server mod_proxy Reverse代理模式安全限制绕过漏洞	11
MySQL多个版本资源管理错误漏洞	1
MySQL Item_singlerow_subselect::store函数空指针解引用漏洞	1
Apache HTTP Server mod_proxy反向代理模式安全限制绕过漏洞	11
Apache HTTP Server Scoreboard本地安全限制绕过漏洞	11
phpMyAdmin Backtrace存储式跨站脚本漏洞(CVE-2010-2958)	1
phpMyAdmin setup脚本远程跨站脚本漏洞(CVE-2010-3263)	1
Apache HTTP Server “httpOnly” Cookie信息泄露漏洞	11
Apache HTTP Server "mod_proxy"反向代理安全限制绕过漏洞	11
phpMyAdmin 'phpinfo.php'敏感信息泄漏漏洞(CVE-2010-4481)	1
OpenSSH glob表达式拒绝服务漏洞(CVE-2010-4755)	14
Apache HTTP Server suexec 任意文件创建漏洞(CVE-2007-1743)	2
phpMyAdmin数据库搜索跨站脚本执行漏洞	1
Apache HTTP Server 'LD_LIBRARY_PATH'不安全库加载任意代码执行漏洞	13
Apache mod_proxy_ftp模块跨站脚本执行漏洞	2
Oracle MySQL Server远程拒绝服务漏洞(CVE-2012-0102)	1
MySQL 企业服务版绕过权限查询漏洞	1
Apache HTTP Server拒绝服务漏洞	5
Apache Tomcat Slowloris工具拒绝服务漏洞	1

漏洞名称	出现次数
Apache HTTP Server日志内终端转义序列命令注入漏洞	14
Apache Tomcat FORM认证器会话固定漏洞(CVE-2013-2067)	1
远端WWW服务支持TRACE请求	8
MySQL Rename Table函数访问验证漏洞	1
可移植OpenSSH GSSAPI认证终止信息泄露漏洞	1
MySQL MyISAM表绕过权限检查漏洞	1
猜测出远程FTP服务存在可登录的用户名口令	1
Apache HTTP Server AllowOverride选项绕过安全限制漏洞	3
MySQL SELECT语句处理拒绝服务漏洞	1
MySQL畸形报文处理远程拒绝服务漏洞	1
Apache HTTP Server mod_cache和mod_dav模块远程拒绝服务漏洞	9
ISC BIND 9递归查询远程拒绝服务漏洞	2
ISC BIND 9 "RRSIG"记录类型否定响应缓存远程拒绝服务漏洞	2
ISC BIND 9 密钥更新安全漏洞	2
ISC BIND安全限制绕过漏洞	3
phpMyAdmin libraries/bookmark.lib.php PMA_Bookmark_get函数输入验证漏洞	1
Apache 未定义字元编码跨站漏洞	2
Apache mod_proxy_balancer拒绝服务漏洞	2
Apache mod_proxy_balancer模块多个跨站脚本漏洞	2
Oracle MySQL 存在拒绝服务漏洞	1
Oracle MySQL Server远程拒绝服务漏洞(CVE-2012-0087)	1
Apache ARP libray远程拒绝服务漏洞	3
Apache mod_proxy_ajp模块入站请求消息远程拒绝服务漏洞	5
Apache子请求处理信息泄露漏洞（CVE-2010-0434）	5
Apache HTTP Server远程拒绝服务漏洞(CVE-2013-1896)	14
vsftpd FTP Server 'ls.c' 远程拒绝服务漏洞(CVE-2011-0762)	3
ISC BIND 9 Large RRSIG RRsets远程拒绝服务漏洞(CVE-2011-1910)	2
phpMyAdmin多个安全漏洞(CVE-2011-2505)	1
phpMyAdmin多个安全漏洞(CVE-2011-2507)	1
phpMyAdmin多个安全漏洞(CVE-2011-2508)	1
Apache Portable Runtime和HTTP Server 'fnmatch()'栈消耗漏洞(CVE-2011-0419)	11
phpMyAdmin多个跨站脚本漏洞(CVE-2010-3056)	1
phpMyAdmin多个脚本插入漏洞(CVE-2011-3181)	1
Apache mod_tcl远程格式串处理漏洞(CVE-2006-4154)	2
Microsoft IIS 安全扩展名输入验证漏洞(CVE-2009-4445)	4
Microsoft IIS畸形文件扩展名绕过安全限制漏洞（CVE-2009-4444）	4

漏洞名称	出现次数
Portable OpenSSH 'ssh-keysign'本地未授权访问漏洞	15
phpMyAdmin脚本注入漏洞	1
nginx 'ngx_http_close_connection()'远程整数溢出漏洞	1
ISC BIND 9 SRTT算法授权服务器选择安全漏洞	2
OpenSSH S/Key 远程信息泄露漏洞(CVE-2007-2243)	5
Apache htpasswd密码salt值生成不随机漏洞	2
Apache HTTP Server多个拒绝服务漏洞(CVE-2013-6438)	15
Apache HTTP Server多个拒绝服务漏洞(CVE-2014-0098)	15
PHP "gdImageCreateFromXpm()"空指针间接引用漏洞(CVE-2014-2497)	1
Apache Tomcat 输入验证漏洞(CVE-2013-4322)	1
OpenSSH 权限许可和访问控制漏洞(CVE-2014-2532)	16
Apache Tomcat 输入验证漏洞(CVE-2013-4286)	1
Oracle MySQL Client远程安全漏洞(CVE-2014-2440)	1
Oracle MySQL Server远程安全漏洞(CVE-2014-2419)	1
Oracle MySQL Server远程安全漏洞(CVE-2014-2436)	1
Oracle MySQL Server远程安全漏洞(CVE-2014-0384)	1
Apache Tomcat 块请求远程拒绝服务漏洞（CVE-2014-0075）	2
PHP 'cdf_read_property_info()'函数拒绝服务漏洞（CVE-2014-0238）	1
PHP 'cdf_unpack_summary_info()'函数拒绝服务漏洞（CVE-2014-0237）	1
Apache Tomcat 权限许可和访问控制漏洞(CVE-2014-0119)	2
Apache Tomcat 权限许可和访问控制漏洞(CVE-2014-0096)	2
Apache Tomcat 整数溢出漏洞(CVE-2014-0099)	2
PHP 安全漏洞(CVE-2014-4721)	1
PHP ‘unserialize()’ 函数类型混淆安全漏洞(CVE-2014-3515)	1
PHP Fileinfo组件'cdf_count_chain()'函数远程拒绝服务漏洞（CVE-2014-3480）	1
PHP Fileinfo组件远程拒绝服务漏洞（CVE-2014-3478）	1
PHP Fileinfo组件 ‘cdf_read_short_sector’ 函数缓冲区溢出漏洞（CVE-2014-0207）	1
Oracle MySQL Server 远程安全漏洞(CVE-2014-4258)	1
Oracle MySQL Server 远程安全漏洞(CVE-2014-4260)	1
Oracle MySQL Server 远程安全漏洞(CVE-2014-2494)	1
Oracle MySQL Server 远程安全漏洞(CVE-2014-4207)	1
Apache HTTP Server远程拒绝服务漏洞(CVE-2014-0231)	1
Apache HTTP Server远程拒绝服务漏洞(CVE-2014-0118)	1
Apache HTTP Server远程拒绝服务漏洞(CVE-2014-3523)	1

漏洞名称	出现次数
Apache HTTP Server 'mod_status'远程代码执行漏洞(CVE-2014-0226)	1
PHP多个任意文件覆盖漏洞（CVE-2014-5120）	1
Apache Tomcat 输入验证漏洞(CVE-2014-0033)	1
PHP 'cdf_read_property_info()' 函数拒绝服务漏洞（CVE-2014-3587）	1
PHP DNS TXT记录处理堆缓冲区溢出漏洞（CVE-2014-3597）	1
Oracle MySQL Client yaSSL证书解码缓冲区溢出漏洞	1
SSL 3.0 POODLE攻击信息泄露漏洞(CVE-2014-3566)【原理扫描】	3
Apache HTTP Server mod_headers模块权限许可和访问控制漏洞(CVE-2013-5704)	3
OpenSSH verify_host_key函数 SSHFP DNS RR 检查绕过漏洞(CVE-2014-2653)	16
Apache HTTP Server mod_cache拒绝服务漏洞(CVE-2014-3581)	1
Apache Tomcat XML外部实体信息泄露漏洞(CVE-2013-4590)	1
Oracle MySQL Server远程安全漏洞(CVE-2015-0432)	1
Oracle MySQL Server远程安全漏洞(CVE-2015-0382)	1
Oracle MySQL Server远程安全漏洞(CVE-2015-0391)	1
Oracle MySQL Server远程安全漏洞(CVE-2015-0381)	1
PHP释放后重利用远程代码执行漏洞(CVE-2015-0273)	1
Apache HTTP Server mod_lua模块输入验证漏洞(CVE-2015-0228)	15
Apache Tomcat 安全漏洞(CVE-2014-0227)	2
ISC BIND远程拒绝服务漏洞(CVE-2015-1349)	3
SSL/TLS 受诫礼(BAR-MITZVAH)攻击漏洞(CVE-2015-2808)【原理扫描】	3
PHP 'libxmlrpc/xmlrpc.c'缓冲区溢出漏洞(CVE-2014-3668)	1
PHP GD 缓冲区溢出漏洞(CVE-2014-9709)	1
PHP move_uploaded_file 权限许可和访问控制漏洞(CVE-2015-2348)	1
PHP Fileinfo组件 ‘cdf_read_property_info()’ 函数拒绝服务漏洞(CVE-2014-3487)	1
PHP 'exif_process_unicode()'函数远程代码执行漏洞(CVE-2015-0232)	1
PHP Fileinfo组件file 缓冲区溢出漏洞(CVE-2014-9652)	1
Oracle MySQL Server Server:Security:Privileges子组件拒绝服务漏洞(CVE-2015-2568)	2
Oracle MySQL Connectors组件安全漏洞(CVE-2015-2575)	1
Oracle MySQL Server Server:Information Schema子组件拒绝服务漏洞(CVE-2015-0500)	2
Oracle MySQL Server Server:InnoDB:DML 拒绝服务漏洞(CVE-2015-0433)	2

漏洞名称	出现次数
Oracle MySQL Server Server:Optimizer子组件拒绝服务漏洞(CVE-2015-0423)	2
Oracle MySQL Server Server:Optimizer子组件拒绝服务漏洞(CVE-2015-2571)	2
Oracle MySQL Server Server:Partition 拒绝服务漏洞(CVE-2015-0438)	2
Apache Tomcat拒绝服务漏洞(CVE-2014-0230)	2
PHP PostgreSQL扩展拒绝服务漏洞(CVE-2015-1352)	1
Oracle MySQL SSL证书验证安全限制绕过漏洞(CVE-2015-3152)	2
Apache Tomcat Security Manager绕过漏洞(CVE-2014-7810)	2
PHP PHAR 'phar_tar_process_metadata()'函数堆内存破坏漏洞(CVE-2015-3307)	1
PHP OS命令注入漏洞(CVE-2015-4642)	1
检测到远端rpc.nlockmgr服务正在运行中	4
目标主机showmount -e信息泄露	4
可通过HTTPS获取远端WWW服务信息	3
远程代理服务器接受POST请求	1
存在一个可用的远程代理服务器	1
POP3服务器的类型和版本泄漏	2
SSH版本信息可被获取	17
Microsoft SQL Server数据库服务正在运行	1
远程主机允许匿名FTP登录	1
FTP服务器版本信息可被获取(CVE-1999-0614)	4
远端WEB服务器上存在/robots.txt文件	1
可通过HTTP获取远端WWW服务信息	18
远程MySQL/MariaDB Server版本泄露	4
远端运行着BIND 9.x	3
可以获取远端Symantec AntiVirus部分信息	1
检测到远端Symantec AntiVirus正在运行中	1
Apache Tomcat NIO连接器拒绝服务漏洞	1
远端SSH Server允许使用低版本SSH协议	1
IBM DB2 'Common Code Infrastructure'组件安全绕过漏洞	1
目标主机rpcinfo -p信息泄露	1
Windows终端服务器通信加密级别检查	1
IMAP服务信息可被获取	2
Oracle MySQL Server本地访问安全漏洞(CVE-2012-0114)	1
MySQL命令行客户端HTML注入漏洞	1
OpenSSH X11UseLocalhost X11转发会话劫持漏洞(CVE-2008-3259)	5

漏洞名称	出现次数
Apache HTTP Server mod_negotiation HTTP响应分裂漏洞(CVE-2008-0456)	2
OpenSSH auth_parse_options函数信任管理漏洞(CVE-2012-0814)	15
MySQL MyISAM表格符号链接本地权限提升漏洞(CVE-2012-4452)	1
Apache mod_proxy_ftp模块空指针引用拒绝服务漏洞	3
检测到目标服务支持SSL中等强度加密算法	2
检测到目标主机加密通信支持的加密算法	3
phpMyAdmin 3.3.10.3和3.4.3.2之前版本多个远程漏洞(CVE-2011-2642)	1
Oracle MySQL 5.1.52之前版本多个拒绝服务漏洞	1
Oracle MySQL Server远程未明细节安全漏洞(CVE-2012-0075)	1
Apache HTTP Server mod_log_config拒绝服务漏洞	2
Apache HTTP Server suexec 权限许可和访问控制漏洞(CVE-2007-1742)	2
OpenBSD OpenBSD OpenSSH 信任管理漏洞(CVE-2005-2666)	1
Apache mod_proxy_balancer模块跨站脚本执行漏洞	2
允许Traceroute探测	29
SMTP服务器版本信息可被获取	3
检测到远端rpc.yppasswdd服务正在运行中	1
检测到远端rpc.mountd服务正在运行中	4
检测到远端RPCBIND/PORTMAP正在运行中(CVE-1999-0632)	8
检测到远端DNS服务正在运行中	3
检测到远端XFS服务正在运行中	1
检测到目标主机上运行着NTP服务	7
检测到远端rpc.nfsd服务正在运行中	4
检测到远端rpc.rquotad服务正在运行中	3
检测到远端rpc.statd服务正在运行中	6
远程代理服务器允许连接任意端口	1
检测到远端LDAP服务正在运行中	1
远端DNS服务允许区传输操作	3
可获取远端BIND服务的版本信息	3
ICMP timestamp请求响应漏洞	30
Oracle MySQL Server两个不明细节本地漏洞	1
Apache HTTP Server “ap_pregsub()”函数拒绝服务漏洞	11
Apache HTTP Server 'ap_pregsub()'函数本地拒绝服务漏洞	11
OpenSSH 'ssh_gssapi_parse_ename()'函数拒绝服务漏洞	15
检测到PPTP服务	1
ISC BIND ‘query_findclosestnsec3’函数缓冲区溢出漏洞(CVE-2014-0591)	3

漏洞名称	出现次数
OpenSSH 信息泄露漏洞(CVE-2011-4327)	15
phpMyAdmin import.php 跨站脚本漏洞(CVE-2014-1879)	2
WordPress 服务检测	1
Oracle MySQL Server远程安全漏洞(CVE-2014-2430)	1
Oracle MySQL Server远程安全漏洞(CVE-2014-2438)	1
Oracle MySQL Server远程安全漏洞(CVE-2014-2432)	1
Oracle MySQL Server远程安全漏洞(CVE-2014-2431)	1
Sendmail 信息泄露漏洞(CVE-2014-3956)	1
Oracle MySQL Server 远程安全漏洞(CVE-2014-4243)	1
Oracle MySQL Server远程安全漏洞(CVE-2015-0374)	1
Oracle MySQL Server远程安全漏洞(CVE-2014-6568)	1
PHP Pear '/tmp/'Directory 安全漏洞(CVE-2014-5459)	1
Oracle MySQL Server Server:DDL子组件拒绝服务漏洞(CVE-2015-0505)	2
Oracle MySQL Server Server:InnoDB子组件拒绝服务漏洞(CVE-2015-0506)	2
Oracle MySQL Server Server:Security:Privileges子组件拒绝服务漏洞(CVE-2015-2567)	2
Oracle MySQL Server Server:Replication子组件拒绝服务漏洞(CVE-2015-0498)	2
合计	**910**

脆弱帐号

SMB帐号 [0]

应用程序帐号 [3]

IP地址	用户名	密码	应用程序
159.226.88.35	anonymous	anon@ymous.tw	FTP Server
159.226.88.35	ftp	(任意密码)	FTP
159.226.88.60	root	root	MySQL

Unix帐号 [0]

参考标准

单一漏洞风险等级评定标准

危险程度	危险值区域	危险程度说明
高	7 <= 漏洞风险值 <= 10	攻击者可以远程执行任意命令或者代码，或进行远程拒绝服务攻击。
中	4 <= 漏洞风险值 < 7	攻击者可以远程创建、修改、删除文件或数据，或对普通服务进行拒绝服务攻击。
低	0 <= 漏洞风险值 < 4	攻击者可以获取某些系统、服务的信息，或读取系统文件和数据。
分值	评估标准	

1	可远程获取OS、应用版本信息。
2	开放了不必要或危险的服务，可远程获取系统敏感信息。
3	可远程进行受限的文件、数据读取。
4	可远程进行重要或不受限文件、数据读取。
5	可远程进行受限文件、数据修改。
6	可远程进行受限重要文件、数据修改。
7	可远程进行不受限的重要文件、数据修改，或对普通服务进行拒绝服务攻击。
8	可远程以普通用户身份执行命令或进行系统、网络级的拒绝服务攻击。
9	可远程以管理用户身份执行命令（受限、不太容易利用）。
10	可远程以管理用户身份执行命令（不受限、容易利用）。

主机风险等级评定标准

主机风险等级	主机风险值区域
非常危险	7 <= 主机风险值 <= 10
比较危险	5 <= 主机风险值 < 7
比较安全	2 <= 主机风险值 < 5
非常安全	0 <= 主机风险值 < 2

1.将主机的漏洞按照分数的高低排序，依据漏洞的分数将漏洞威胁划分为高、中、低三个类别。
2.按照 绿盟科技 风险评估模型计算得到风险值。

注：高、中和低漏洞威胁的定义参见《单一漏洞风险等级评定标准》

网络风险等级评定标准

网络风险等级	网络风险值区域
非常危险	8 <= 网络风险值 <= 10
比较危险	5 <= 网络风险值 < 8
比较安全	1 <= 网络风险值 < 5
非常安全	0 <= 网络风险值 < 1

网络风险等级是网络中所有主机威胁分值的加权平均和。
1 对网络中的所有主机按照威胁分值进行高低排序，依据主机的威胁分值将主机风险划分为高、中、低三
2.按照 绿盟科技 风险评估模型计算得到风险值。

其中：
非常危险的主机定义为高风险；比较危险的主机定义为中风险；比较安全和非常安全的主机定义为低

安全建议

据市场研究公司 Gartner 研究报告称“实施漏洞管理的企业会避免近 90% 的攻击”。可以看出，及时的漏洞修补可以在一定程度上防止病毒、攻击者的威胁。

绿盟科技“远程安全评估系统”建议对存在漏洞的主机参考附件中提出的解决方案进行漏洞修补、安全增强。

- 建议所有 Windows 系统使用“Windows Update”进行更新。
- 对于大量终端用户而言，可以采用 WSUS 进行自动补丁更新，也可以采用补丁分发系统及时对终端用户进行补丁更新。
- 对于存在弱口令的系统，需在加强使用者安全意识的前提下，督促其修改密码，或者使用策略来强制限制密码长度和复杂性。
- 对于存在弱口令或是空口令的服务，在一些关键服务上，应加强口令强度，同时需使用加密传输方式，对于一些可关闭的服务来说，建议关闭该服务以达到安全目的。
- 对于UNIX系统订阅厂商的安全公告，与厂商技术人员确认后进行漏洞修补、补丁安

装、停止服务等。

- 由于其他原因不能及时安装补丁的系统，考虑在网络边界、路由器、防火墙上设置严格的访问控制策略，以保证网络的动态安全。
- 建议网络管理员、系统管理员、安全管理员关注安全信息、安全动态及最新的严重漏洞，攻与防的循环，伴随每个主流操作系统、应用服务的生命周期。
- 建议采用绿盟科技的“冰之眼”网络入侵检测系统实时监控网络流量，及时发现病毒感染源。
- 建议采用绿盟科技“远程安全评估系统”定期对网络进行评估，真正做到未雨绸缪。
