



网络通讯协议图2022版

Network Communication Protocols Map



科来·全球领先的网络流量分析企业

科来成立于2003年，是专注于网络流量分析技术研究与产品开发的高新技术企业，在这一领域有着几十项专利技术和完全独立的自主知识产权。科来研发的产品广泛应用于国内外用户的网络智能运维与网络安全分析等关键领域。

科来于2010年在国内率先提出“全流量”、“回溯”概念，并推出了以网络全流量采集与分析技术为基础的网桥回溯产品。科来形成了面向政府、金融、能源、运营商、交通等不同行业、不同规模、不同需求的解决方案。是国内最有影响力的数据分析技术提供商。

由于科来公司在网络安全领域的技术优势，受邀为“建国72周年”、“中国海军成立70周年”阅兵活动、“军运会”、“中非合作论坛”峰会、青岛“上合峰会”、“多国”、“十九大”、“杭州G20峰会”、“世界田径锦标赛”、多届“数博会”等重大国家政治使团和相关工作，做出突出贡献。

科来专注于数据价值，始终秉承着“坚持、责任、进取”的理念。艾媒把用户数据价值发挥到最大化，通过数据驱动运维、数据驱动安全、数据驱动管理，进一步提升运维自动化能力，帮助企业解决数据问题和分析的基础上应对日益严峻的网络安全和运维风险。

科来荣誉



• 科来蝉联Gartner NPM魔力象限“远见者”称号

2018-2019年，科来蝉联Gartner NPM魔力象限“远见者”称号，是唯一入选该报告的中国企业。根据Gartner NPM魔力象限报告，定义科来为“通过数据包分析技术实现网络关键性能指标可标记来简化网络运维”。

• Gartner NPM魔力象限指南，科来是代表性供应商中唯一被详细介绍的中国企业

Gartner发布2020年NPM市场指南，该指南对NPM市场做了权威分析，并挑选出20家厂商进行详细介绍。作为代表供应商，科来是该报告中唯一被详细介绍的中国企业。

• 科来蝉联中国NPAM领域市场占有率第一，遥遥领先

根据全球权威调研与咨询机构IDC发布《China Semiannual IT Unified Operation Software Tracker》报告，科来连续多年位居中国网络性能分析管理领域榜首，市场占有率达到领先地位。

用户认可



科来在全球

产品覆盖全球 110 个国家和地区，拥有 10000 余家商业客户，超过 134 家世界 500 强企业选择科来。



科来全球用户



科来CSNA网络分析认证培训

让更多人掌握高级网络分析技术，为国家培养更多网络分析人才

科来于2015年开始了CSNA网络分析认证培训。该培训基于科来对网络协议的独到见解和行业十余年的真实经验累积，对专业性、实操性、实用性都有极深的研究和积累。学员通过培训，能够熟练掌握网络分析技术，同时掌握解决90%以上的网络安全与威胁安全问题的思路。CSNA网络分析认证培训开办至今已经培养了上万优秀的网络分析技术人才，学员广泛就职于关系国计民生行业的重点岗位。



详情请通过科来微信公众号、官网www.colosoft.com.cn或致电400-6009-099垂询。

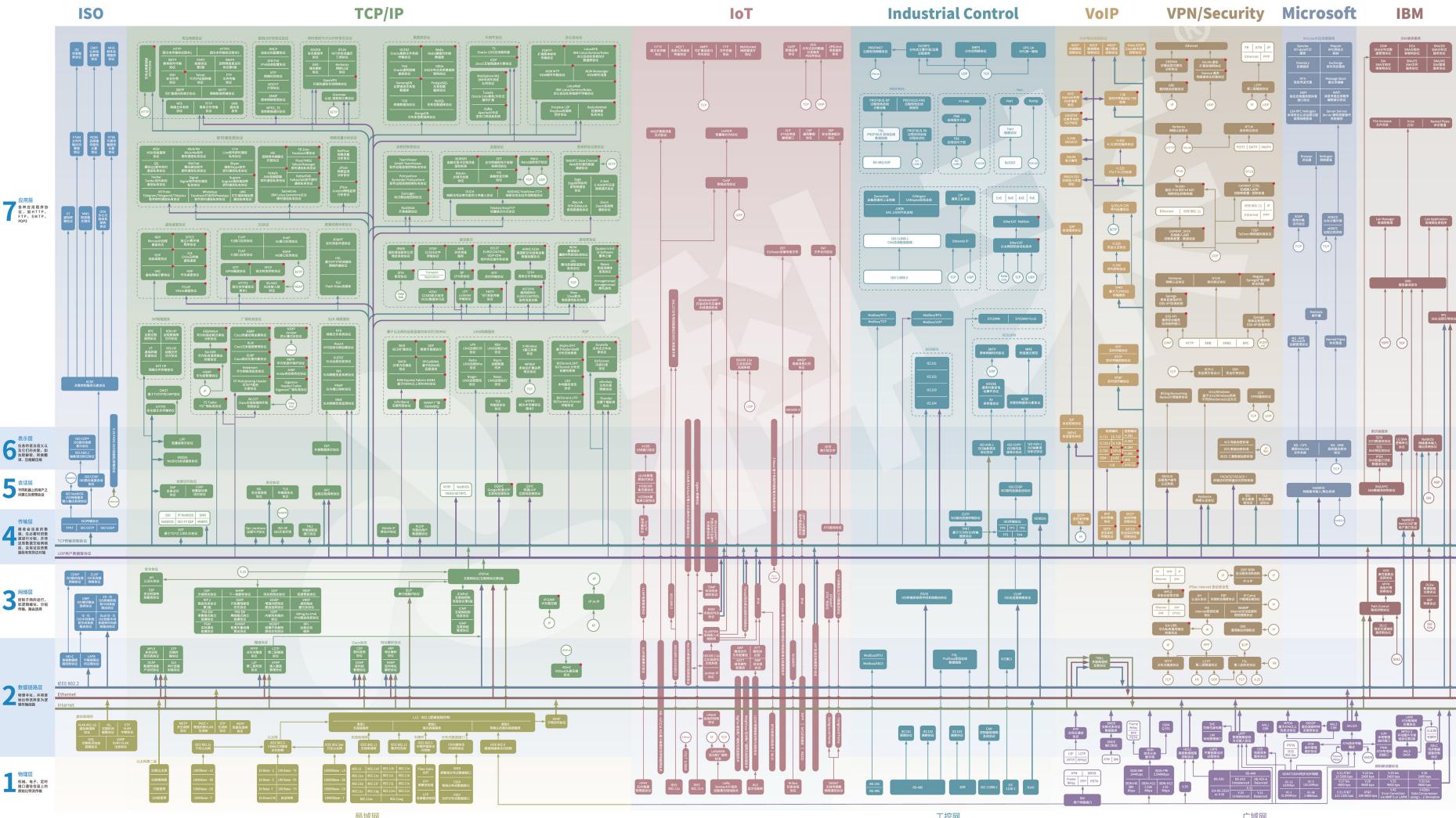


客服电话：400 6009 099
官方网站：www.colosoft.com.cn

©2018-2022 科来公司版权所有。保留所有权利。

此产品仅限于实验室、测试、教育及学术研究使用。

本产品仅限于实验室、测试、教育及学术研究使用。本公司不对未经授权产生的收益。



TCP/IP协议簇常见协议信息

协议	RFC 编号	端口	OSI 层次	协议	RFC 编号	端口	OSI 层次
AH	RFC 2402		网络层	NNTP	RFC 977	TCP/UDP-119	数据链路层
ARP	RFC 826		数据链路层	NTP	RFC 958	TCP/UDP-123	数据链路层
ATMP	RFC 2107		数据链路层	OSPF	RFC 2178,2328		网络层
BGP	RFC 4271	TCP/UDP-179	应用层	PGM	RFC 3308		网络层
BGPP0T	RFC 951	UDP-67,UDP-68	应用层	PIM-DM	RFC 2673		网络层
COPS	RFC 2748	TCP/UDP-32888	数据链路层	PIM-SM	RFC 2362		网络层
DCAP	RFC 2114		应用层	POPS	RFC 1938	TCP-110	应用层
DHCP	RFC 2131	UDP-67,UDP-68,UDP-4311	应用层	PTP	RFC 2637	TCP/UDP-1723	数据链路层
DNS	RFC 4343	TCP/UDP-53,TCP/UDP-1993	应用层	PostgreSQL		TCP/UDP-5432	应用层
DNSA	TCP-50000		应用层	Radius	RFC 2138	TCP/UDP-1812	应用层
DummengDB	TCP-5238		应用层	RARP	RFC 903		数据链路层
DVMRP	RFC 1075		网络层	RIP2	RFC 2453		网络层
ESP	RFC 2406		网络层	RIPng for IPv6	RFC 2680		网络层
FANP	RFC 2129		应用层	RLDGIN	RFC 1258,1282	TCP-513	应用层
finger	RFC 1194,1196,1228	TCP/UDP-79	应用层	RPC	RFC 1050,1053,1831	TCP/UDP-111	会话层
FTP	RFC 955	TCP-20,TCP-21	应用层	RSPV	RFC 2205,2750	TCP/UDP-545	网络层
HTTP	RFC 1945,2616	TCP-80	应用层	RTSP	RFC 2236	TCP/UDP-554	应用层
IARP	RFC 2300		数据链路层	RUDP	RFC 906,1151		传输层
ICMP	RFC 792		网络层	REDIS	TCP-6379		应用层
ICMPv6	RFC 1885,2463		网络层	SCTP	RFC 2960	TCP-9036	传输层
ICP	RFC 2186	TCP-29	应用层	S-HTTP	RFC 2660	TCP-443	应用层
IGMP	RFC 1112,2336,3316		网络层	SIP	RFC 1055		网络层
IMAP4	RFC 3733	TCP-143	应用层	SIP	RFC 2365	TCP/UDP-427	应用层
iSCSI	RFC 3120	TCP/UDP-860	应用层	SMTP	RFC 821,2821	TCP/UDP-25	应用层
IP	RFC 791		网络层	SNMP	RFC 1157	TCP/UDP-161,UDP-162	应用层
IPv6	RFC 1883,2460		网络层	SOCKS	RFC 1928	TCP/UDP-1081	会话层
IRC	RFC 1459	TCP/UDP-194	应用层	TACACS	RFC 1492	TCP/UDP-49	应用层
ISAKMP	RFC 2048	TCP/UDP-500	应用层	TALI	RFC 3694	TCP/UDP-49	传输层
L2F	RFC 2341	TCP/UDP-1701	数据链路层	TCP	RFC 793		传输层
L2TP	RFC 2661	TCP/UDP-1701	数据链路层	TOS		TCP/UDP-1433	应用层
LDAP	RFC 1777	TCP/UDP-389	会话层	TOS		TCP/UDP-1521	应用层
LDP	RFC 108		会话层	TELNET	RFC 854	TCP/UDP-23	应用层
MARS	RFC 2022		网络层	TFTP	RFC 1350	TCP/UDP-69	应用层
Mobile IP	RFC 2002	UDP-434	传输层	TLS	RFC 2246	TCP-443	会话层
MSDP	RFC 1585		网络层	UDP	RFC 768		传输层
MPLS	RFC 3631,3032		数据链路层	Van Jacobson	RFC 1144		传输层
MySQL	TCP/UDP-3306		应用层	VRRP	RFC 2338,3168		网络层
MongoDB	TCP-27017		应用层	XOT	RFC 1613	TCP/UDP-1996	传输层
NBNS/B	RFC 1001,1002	TCP/UDP-1314,1319	会话层	X-Window	RFC 1158	TCP/UDP-6005	应用层
NHRP	RFC 2332		网络层	XMPP	RFC 3920	TCP/UDP-5198	应用层

常见协议漏洞信息

基于常见协议且危险程度为高危的软件漏洞信息

协议	软件	漏洞编号	漏洞描述
BitTorrent	BitTorrent	CVE-2020-8437	BitTorrent uTorrent Bencode 解析器没有正确解析使用Bencode编码方式的嵌入式字典
IIOP	Bitcoin Core	CVE-2019-15947	Bitcoin Core 加密问题漏洞
Bitcoin Core/Bitcoin Knots	Bitcoin Core/Bitcoin Knots	CVE-2018-17344	Bitcoin Core/Bitcoin Knots 插入验证错误漏洞
Cisco Discovery	Cisco IOS XR Software	CVE-2020-3118	Cisco IOS XR Software 对以太网中某些字节的输入输出不当导致远程代码执行漏洞
DHCP	Microsoft Windows	CVE-2019-0726	Windows DHCP 操作系统没有正常处理内存中对象导致了远程代码执行漏洞
DHCP	Microsoft Windows	CVE-2019-0547	Windows DHCP 客户端存在内存损坏漏洞
DNS	PostgreSQL	TCP/UDP-5432	PostgreSQL 对SQL命令使用的特殊元转义处理不当导致SQL注入
DNSA	Radius	TCP/UDP-1812	Radius 对SQL命令使用的特殊元转义处理不当导致SQL注入
DwarfedDB	RARF	RFC 903	数据链路层
EAP	PPP	CVE-2020-8597	PPP 框压包由远程代码执行漏洞
EAP	FTT-Srv	CVE-2020-15152	FTT-Srv 特权用户通过请求服务器重置会话造成远程代码执行漏洞
EAP	Cisco Web Security Appliance	CVE-2018-0087	Cisco Web Security Appliance FTP Server 身份验证不当漏洞
EAP	AKP-Tools	CVE-2021-36159	FreeRADIUS LDAP 身份验证漏洞
EAP	Wing FTP Server	CVE-2020-9470	Wing FTP Server 中的本地权限提升
EAP	Wing FTP Server	CVE-2020-8635	Wing FTP Server 中的恶意 Wing FTP 配置文件不安全的权限利用
EAP	HAXX1 libcurl	CVE-2020-8285	恶意 FTP 服务器可以在使用 CURLOPT_CHUNK_BGN_FUNCTION 和 CURLOPT_READFUNCTION 时触发堆溢出漏洞
EAP	Apache Log4j	CVE-2021-45105	Apache Log4j 新功能堆溢出漏洞
EAP	Apache Tomcat	CVE-2020-1938	Tomcat API 处理请求时包含漏洞 Tomcat 链接头漏洞
EAP	Nagios Network Analyzer	CVE-2013-28925	Nagios Network Analyzer SQL 命令中使用的特殊元素转义处理不恰当
EAP	The ApacheOpen For Business Project	CVE-2013-28295	The ApacheOpen For Business Project 反序列化任意代码执行漏洞
EAP	HTTP 特权连接	CVE-2021-31166	HTTP 特权连接远程代码执行漏洞
EAP	Microsoft Exchange Server	CVE-2021-27065	Microsoft Exchange Server 允许设置文件名和路径导致文件写入漏洞
EAP	F5 Networks	CVE-2020-5902	F5 BIG-IP 配置不当和之后身份验证导致远程代码执行漏洞
EAP	Drupal	CVE-2018-7609	Drupal 表单参数未正确验证导致远程代码执行漏洞
EAP	Apache Solr	CVE-2017-12839	Apache Solr 外部字体库绕过命令执行漏洞
EAP	Apache Tomcat	CVE-2017-12637	Apache Tomcat PUT 文件上传漏洞
EAP	Microsoft Windows	CVE-2022-23907	HTTP 特权连接远程代码执行漏洞
EAP	F5 Networks	CVE-2021-22886	F5 BIG-IP iControl REST 未授权远程代码执行漏洞
EAP	D-Link	CVE-2019-16920	D-Link 会议令牌注入漏洞
EAP	Microsoft SharePoint	CVE-2019-0604	Microsoft SharePoint 签名验证不当导致远程代码执行漏洞
EAP	Fortinet Fortigate	CVE-2018-13379	Fortigate SSL VPN 会话劫持漏洞
EAP	Citrix Application Delivery Controller	CVE-2019-19783	Citrix ADC 为凭据身份验证的远程攻击者在目标服务器上执行命令
EAP	Apache Shiro	CVE-2016-4437	Apache Shiro 账户密钥命令执行漏洞
HTTP	Apache Tomcat	CVE-2020-11996	Apache Tomcat 资源清理漏洞
HTTP	Nginx	CVE-2018-16644	Nginx 在 HTTP 的实现中存在一个允许 CPU 占用过高的漏洞
HTTP	Apache HTTP Server	CVE-2016-8740	Apache HTTP Server 本地权限漏洞
HTTP	Apache Tomcat	CVE-2020-17527	Apache Tomcat 信息泄露漏洞
HTTP2	Apache Tomcat	CVE-2018-10598	PostgreSQL 函数参数可导致远程代码执行漏洞
HTTP2	PostgreSQL	CVE-2018-21724	PostgreSQL JDBC 读取内存代码执行漏洞
HTTP2	PostgreSQL	CVE-2019-19193	PostgreSQL 任意代码执行漏洞
ICMP	Apple	CVE-2019-8605	IDS 内核地址劫持漏洞
ICMP	Apple Mac OS Sierra	CVE-2018-4407	Apple Mac OS Sierra 代码执行漏洞
IDAP/HTTP	Apache Log4j	CVE-2021-44228	Apache Log4j lookup 功能插入前缀不当导致远程代码执行漏洞
ICMP	Telnet	CVE-2017-22925	Telnet 在将未初始化的数据从基于堆栈的缓冲区发送到服务器的漏洞
ICMP	Netkit Telnet	CVE-2010-10188	Netkit Telnet 在没有世界写权限并允许远程执行代码
ICMP	Telnet	CVE-2013-7555	TX9 Automatic Food Dispenser 未经授权管理权限漏洞
ICMP	Rubetek Camera	CVE-2010-25169	Rubetek RV-3406 Firmware 未经授权的权限漏洞
ICMP	Rubetek Camera	CVE-2010-25174	Rubetek RV-3406 Firmware 未经授权的权限漏洞
ICMP	Juniper Networks Junos OS	CVE-2019-0058	Juniper Networks Junos OS 未经授权读取漏洞
ICMP	Cisco IOS/Cisco IOS XE	CVE-2017-8881	多线程攻击导致远程代码执行漏洞
ICMP	Microsoft Windows	CVE-2011-145	Windows SMBv1 Server 组件上存在远程代码执行漏洞
ICMP	Microsoft Windows	CVE-2011-1432	Windows SMB 大部分连接上存在远程代码执行漏洞
ICMP	Microsoft Server Message Block	CVE-2012-0796	Microsoft Windows SMBv3 插入验证错误漏洞
ICMP	Samba	CVE-2021-4142	Samba 本地权限提升漏洞
ICMP	OpenSsh	CVE-2018-6789	Exim+PSMT 读取命令执行漏洞
ICMP	OpenSsh	CVE-2020-8794	OpenSsh mta_ia 读取命令执行命令行漏洞
ICMP	OpenSsh	CVE-2020-2747	OpenSsh mta_ia 读取命令执行命令行漏洞
ICMP	Atlasian Jira	CVE-2013-1581	Atlasian Jira SMTP 版本低代码执行漏洞
ICMP	Cisco IOS/Cisco IOS XE	CVE-2017-6744	Cisco IOS/XE SNMP 系统中的缓冲区溢出漏洞
ICMP	B&R Automation Runtime	CVE-2019-1910	SNMP 服务中的身份验证漏洞
ICMP	Cisco IOS/Cisco IOS XE	CVE-2017-0742	Cisco IOS/XE SNMP 代理模块远程命令执行漏洞
ICMP	Zoom	CVE-2018-20401	Zoom SNMP Request Credential 未验证管理漏洞
ICMP	CloudView NMS	CVE-2016-5073	CloudView NMS 路由器配置文件攻击
ICMP	Centresys	CVE-2018-15281	Centresys SNMP Trap sql 注入漏洞
ICMP	Cisco IOS/Cisco IOS XE	CVE-2017-0738	Cisco IOS/XE SNMP 代理模块远程命令执行漏洞
ICMP	Castle Rock Computing SNMPc Online	CVE-2020-11557	SNMPc Online 不充分的内存保护机制
ICMP	Cisco IOS/Cisco IOS XE	CVE-2017-6736	Cisco IOS/XE SNMPS子系统缓冲区溢出漏洞
ICMP	Cisco Adaptive Security Appliance	CVE-2016-6366	Cisco Adaptive Security Appliance Software 缓冲区溢出漏洞
ICMP	Microsoft SQL Server	CVE-2020-0618	SQL Server 表表连接远程代码执行漏洞
ICMP	Serv-U	CVE-2013-3521	SolarWinds Serv-U 平台级插入命令缓冲区溢出漏洞
ICMP	OpenSSH	CVE-2021-18041	OpenSSH 代码注入命令缓冲区溢出漏洞
ICMP	OpenSSH	CVE-2016-5515	OpenSSH auth-passwd 命令缓冲区溢出漏洞
ICMP	Libssh	CVE-2020-16301	SSH 存在操作系统命令注入漏洞，导致 Libssh 2.0 会注入漏洞
ICMP	Libssh	CVE-2018-10933	Libssh 不存在允许没有身份验证的情况下创建连接，导致了未经授权访问漏洞
ICMP	OpenSSL	CVE-2021-3711	OpenSSL 证书回显漏洞
ICMP	OpenSSL	CVE-2016-12183	SSL/TLS 协议中存在缓冲区溢出漏洞
ICMP	F5 Networks	CVE-2016-5246	F5 BIG-IP (Web) 存在命令注入漏洞
ICMP	OpenSSL	CVE-2016-0800	Oracle Fujitsu M Server 代码注入漏洞
ICMP	Microsoft .NET Framework	CVE-2016-0149	TLS/SSL 信息泄漏漏洞
ICMP	Oracle WebLogic Server	CVE-2020-2555	Weblogic ReflectionExtractor T3 序列化命令执行漏洞
ICMP	Oracle WebLogic Server	CVE-2010-1482	Weblogic LockVersionExtractor T3 序列化不可信赖脚本代码执行漏洞
ICMP	Oracle Fusion Middleware	CVE-2010-2801	Oracle Fusion Middleware WebLogic Server Core 组件存在远程代码执行漏洞
ICMP	Oracle WebLogic Server	CVE-2010-2798	Oracle WebLogic Server 序列化命令注入漏洞
ICMP	Oracle WebLogic Server	CVE-2010-2747	Oracle WebLogic UniversalExtractor T3 序列化漏洞
ICMP	Oracle WebLogic Server	CVE-2010-1465	Weblogic UniversalExtractor T3 序列化命令注入漏洞
ICMP	Oracle WebLogic Server	CVE-2010-13890	Oracle WebLogic Server 启动挂起命令序列化命令注入漏洞
ICMP	Oracle WebLogic Server	CVE-2010-13252	Oracle WebLogic Server 启动挂起命令注入漏洞
ICMP	Oracle WebLogic Server	CVE-2010-13465	Oracle WebLogic Server WLS 序列化命令注入漏洞
ICMP	Oracle WebLogic Server	CVE-2018-3191	Oracle WebLogic Server Iookup 代码注入远程代码执行漏洞
ICMP	Arch Linux	CVE-2010-22925	Telnet 在将未初始化的数据从基于堆栈的缓冲区发送到服务器的漏洞
ICMP	Netkit Telnet	CVE-2010-10188	Netkit Telnet 在没有世界写权限并允许远程执行代码
ICMP	Telnet	CVE-2013-7555	TX9 Automatic Food Dispenser 未经授权管理权限漏洞
ICMP	Rubetek Camera	CVE-2010-25169	Rubetek RV-3406 Firmware 未经授权的权限漏洞
ICMP	Rubetek Camera	CVE-2010-25174	Rubetek RV-3406 Firmware 未经授权的权限漏洞
ICMP	Juniper Networks Junos OS	CVE-2019-0058	Juniper Networks Junos OS 未经授权读取漏洞
ICMP	Cisco IOS/Cisco IOS XE	CVE-2017-8881	多线程攻击导致远程代码执行漏洞