科来

网络通讯协议图2023版

Network Communication Protocols Map

科来-成为全球领先的数字化互联智能时代的守护者

科来成立于2003年，致力于成为全球领先的数字化互联智能时代的守护者，围绕数字化互联智能系统保障的相关技术产品的开发，让数字化互联智能系统更安全、更可靠、更高效。科来在这一领域有着众多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用户的智能运维、安全分析及云网运维等关键领域。

未来，数字化系统越来越多的应用到社会关键基础设施，数字化系统自身的安全、稳定、可靠将至关重要。科来将不懈努力，在为客户创造价值的同时，为整个数字化互联社会的安全和稳定、高效运行增添力量。

- **科来入选《2022年网络安全技术应用试点示范项目》名单**

入选由工信部、国家网信办等共十二部门联合发布的《2022年网络安全技术应用试点示范项目》名单，满足面向公共通信和信息服务、能源、交通、金融等重要行业领域网络安全保障需求。

- **荣获由国家知识产权局颁发的“国家知识产权示范企业”称号**

对自主知识产权技术的持续投入与研究，科来荣获“国家知识产权示范企业”称号，是上级主管部门对于科来依靠自主创新攻克关键技术、取得创新成果的充分肯定。

Gartner

- **科来蝉联Gartner NPMD魔力象限“远见者”称号**

科来蝉联 2018、2019 年 Gartner NPMD 魔力象限“远见者”称号，根据 Gartner NPMD 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视化来简化网络运维”。

- **Gartner NPMD市场指南，科来作为代表性供应商被重点详细介绍**

Gartner 发布 2020、2021 年 NPMD 市场指南，该指南对 NPMD 市场做出了权威分析，并选出 20 家厂商进行详细介绍。科来作为代表性供应商被重点介绍。

IDC

- **科来蝉联中国NPM领域市场占有率第一**

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2018-2022年连续五年位居中国网络性能分析管理领域榜首，超过其他前十总和。

- **科来入选红鲱鱼“全球100强”**

全球知名投资风向杂志《RedHerring》（红鲱鱼）揭晓了2022年度全球百强重量级榜单。科来凭借在网络流量分析技术领域的创新与质量管理，从评选中脱颖而出，一举登榜。

科来能力

科来以自主研发的网络流量分析技术为核心，不断深化产品功能、优化服务，逐步形成了业务性能管理、云网运维、安全分析、工控安全、人才培养、技术服务等业务板块。

▶ 增强数字政府效能

科来提供更敏锐的安全感知与溯源取证能力，让安全问题有据可查，并提高安全处置效率，已得到全国几十家部委、税务、公安、检察院、法院等用户的高度认可。

▶ 加速实现能源行业数字化转型

在石油、石化、电力、煤炭、新型能源能众多用户均采用了科来的流量分析解决方案，实现了全网集中统一管理与展现，提高整体运维质量，保障关键业务运行。

▶ 智能交通高质量发展

多个大型航空公司都使用科来的产品提升应用响应速度，在高铁、地铁等进行试点建设，保障交通的通行顺畅。

▶ 科技赋能金融业务

科来同时服务于六大国有银行及全国500余家金融机构，提升了金融行业的核心业务连续性和高可靠性，高精准高性能监测海量订单交易质量，保障每笔支付顺利完成。

▶ 运营商精细化管理与运营保障

科来为三大运营商提供智能化运维保障方案，保障业支、CRM、IT承载网、物联网、5G网络等业务系统的正常运行，为网络、业务与主机的规划和运行管理提供决策依据。

▶ 深化医疗信息化建设

医院业务越来越依赖于网络，科来不仅保障了业务连续性和可靠性，同时还保证医疗数据不被滥用和窃取。

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，培养更多网络分析人才

科来于2005年开办了CSNA网络分析认证培训，该培训是基于科来对网络协议的独到见解与行业内十余年的实战经验累积，对业务性能管理、罕见网络安全事件样本的深度分析总结发展而来。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%以上的网络运维与网络安全问题的思路。CSNA网络分析认证培训开办至今已经培养了众多优秀的网络分析技术人才，学员广泛就业于关系国计民生行业的重要岗位。

专业的服务

“召之即来，战之必胜”。科来在全国部署技术服务力量，可以及时响应用户需求。科来技术服务人员积累了丰富的实战经验，在快速解决问题的同时授人以渔，能够提供更多建设性建议。

多样化、定制化的服务，使科来在政府、金融、能源、运营商、交通、教育、科技、文化、医疗等众多行业用户的服务中获得诸多好评，成为用户持续选择科来的理由。

科来公众号　科来资料　科来视频号

咨询电话：400 6869 069
官方网址：www.colasoft.com.cn

CCPM-2306

科来® 网络通讯协议图2023版

TCP/IP | ISO | IoT | Industrial Control | VoIP | VPN/Security | Microsoft | IBM

7 应用层 各种应用程序协议，如HTTP、FTP、SMTP、POP3

6 表示层 信息的语法语义以及它们的关联，如加密解密、转换翻译、压缩解压缩

5 会话层 不同节点上的用户之间，建立及管理会话

4 传输层 接收会话层数据，在必要时把数据进行分割，并将这些数据交给网络层，且保证这些数据段有效到达对端

3 网络层 控制子网的运行，如逻辑编址、分组传输、路由选择

2 数据链路层 物理寻址，并将原始比特流转变为逻辑传输线路

1 物理层 机械、电子、定时接口通信信道上的原始比特流传输

局域网 | 工控网 | 广域网

关基业务连续运行 · 重要数据安全防护

* 本版更新内容：
在今年的协议图中，TCP/IP模块重点新增卫星通讯协议、无人机协议、半导体SEMI标准协议、RPC框架协议、GB/T38636-2020国密标准TLCP协议、补充4G/5G协议、细化网络层路由协议逻辑；工控模块新增车联网协议、工业以太网系统协议及国家电网标准协议，详细内容请关注图中红色 □ 标识。
将关基安全重点协议框选出，详细内容请关注图中 ▭ 标识。

* 科来为您提供专业的《CSNA网络分析认证培训》服务，服务内容详见科来官网或公众号
* 免费软件、更多学习资料请登录科来官网下载，并双启高校师生教电免费申请印刷版《CSNA网络分析经典实战案例》、《科来网络通讯协议图》及《网络攻击与防范图谱》等资料

科来公众号 | 科来资料 | 科来视频号

咨询电话：400 6869 069
官方网站：www.colasoft.com.cn

TCP/IP协议簇常见协议信息

协 议	引 用	端 口	OSI 层次	协 议	引 用	端 口	OSI 层次
AH	RFC 2402,4302		网络层	NHRP	RFC 2332		网络层
AMQP		TCP-5672	应用层	NTP	RFC 958,1059,1305,5905	UDP-123	应用层
ARP	RFC 826		数据链路层	OpenVPN		UDP-1194	应用层
BGP	RFC 827,2918,4271	TCP-179	网络层	OSPF	RFC 2178,2328,2740 5340,7503		网络层
BitTorrent		TCP-6881~6889	应用层	PFCP	TS 29.244	UDP-8805	应用层
CAPWAP	RFC 5415	UDP-5246,5247	应用层	PGM	RFC 3208		网络层
COAP	RFC 7252,8323	TCP/UDP-5683	应用层	POP3	RFC 1939	TCP-110	应用层
DamengDB		TCP-5236	应用层	PostgreSQL		TCP-5432	应用层
DHCP	RFC 951,1542 2131,2132	UDP-67,68	应用层	Radius	RFC 2138,2865,2866 3162,3576	UDP-1645,1646,1700 1812,1813,3799	会话层
DIAMETER	RFC 3588	TCP/SCTP-3868	应用层	RARP	RFC 903		数据链路层
DNP3	IEEE Std 1815-2010	TCP/UDP-20000	应用层	REDIS		TCP-6379	应用层
DNS	RFC 1035,6762	TCP/UDP-53,5353	应用层	RIP2	RFC 2453	UDP-520	网络层
DRDA		TCP-446~448	应用层	RIPng for IPv6	RFC 2080	UDP-521	网络层
DVMRP	RFC 1075		网络层	RPC	RFC 1050,1057,1831,5531	TCP/UDP-111	会话层
ESP	RFC 2406,4303		网络层	RSVP	RFC 2205,2750	UDP-1698,1699	网络层
FTP	RFC 959	TCP-20,21	应用层	RTSP	RFC 2326,7826	TCP/UDP-554	应用层
GENEVE	RFC 8926	UDP-6081	应用层	RUDP	RFC 908,1151		传输层
GTP	TS 29.060,TS 32.295	UDP-2123,2152 TCP/UDP-3386	应用层	SCTP	RFC 2960,4960,6951	UDP-9899	传输层
GVCP		UDP-3956	应用层	sFlow		UDP-6343	应用层
HTTP	RFC 1945,2616	TCP-80	应用层	SIP	RFC 3261	TCP/UDP/SCTP-5060	应用层
IARP	RFC 2390		数据链路层	SLP(SVRLOC)	RFC 2165,2608	TCP/UDP-427	应用层
ICMP	RFC 792,4884,5837		网络层	SMTP	RFC 821,2821,5321	TCP-25	应用层
ICMPv6	RFC 1885,2463,4443		网络层	SNMP	RFC 1157,3430	UDP-161,162	应用层
ICP	RFC 2186,2187	UDP-3130	应用层	SOCKS	RFC 1928,1929	TCP-1080	会话层
IEC104	IEC 60870-5-104	TCP-2404	应用层	SSH	RFC 4253,4960	TCP-22	应用层
IGMP	RFC 1112, 2236,3376		网络层	STUN	RFC 8489	TCP/UDP-3478	应用层
IMAP4	RFC 1730	TCP-143	应用层	TACACS+	RFC 8907	TCP-49	会话层
IP	RFC 791		网络层	TCP	RFC 793		传输层
IPv6	RFC 1883,2460,8200		网络层	TDS		TCP-1433,2433	应用层
ISAKMP	RFC 2407, 2408 4306,5996	UDP-500,4500	网络层	TELNET	RFC 854,855	TCP-23	应用层
iSCSI	RFC 3720		应用层	TFTP	RFC 1350	UDP-69	应用层
Kerberos	RFC 4120	TCP/UDP-88	会话层	TLS	RFC 2246,4346 5246,8446		会话层
LDAP	RFC 1777,2251,3494 4511,4533	TCP-389	会话层	TNS		TCP-1521	应用层
LLMNR	RFC 4795	TCP/UDP-5355	应用层	TPKT	RFC 983,1006,2126	TCP-102	应用层
MGCP	RFC 2705	UDP-2427,2727	应用层	UDP	RFC 768		传输层
MongoDB		TCP-27017~27020	应用层	VLAN	RFC 3069,IEEE 802.1Q IEEE 802.1ad		数据链路层
MQTT		TCP-1883	应用层	VRRP	RFC 2338,3768		网络层
MySQL		TCP-3306	应用层	VxLAN	RFC 7348	UDP-4789	应用层
NetBIOS	RFC 1001,1002	TCP/UDP-137 TCP-139,UDP-138	会话层	XMPP	RFC 3920,6120		应用层
NFS	RFC 1094,1813,3010,3530 5661,5665,7530	TCP/UDP/SCTP-2049	应用层	X-Window	RFC 1013,1198	TCP-6000~6063	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（图中红色 • 标识为收录的新增漏洞）

协 议	软 件	漏洞编号	漏洞描述
BitTorrent	BitComet	CVE-2022-27050	BitComet Service for Windows存在权限提升漏洞可将权限提升到系统级别
	BitTorrent uTorrent Bencode	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
	Bitcoin Core	CVE-2019-15947	Bitcoin Core 加密问题漏洞
Cisco Discovery	Cisco IOS XR Software	CVE-2020-3118	Cisco IOS XR Software 对协议中某些字段的输入验证不当导致远程代码执行漏洞
DHCP	Microsoft Windows DHCP Client	CVE-2022-37980	Microsoft Windows DHCP Client存在特权提升漏洞
	Open DHCP Server	CVE-2020-26131	攻击者可利用该漏洞，通过替换基于LDAP的根父二进制文件来提升特权
Django	Django	CVE-2021-35042	Django SQL 命令中使用的特殊元素转义处理不恰当导致SQL注入
DNS	Technitium DNS Server	CVE-2022-30258	漏洞源于允许意外域名解析的变体 V2，被撤销的域名在很长一段时间内仍然可以解析
	F5 Networks	CVE-2021-23017	F5 Nginx DNS 解析程序漏洞
	Microsoft Windows DNS Server	CVE-2021-24078	Windows DNS 服务器远程执行漏洞
	Microsoft Windows DNS Server	CVE-2020-1350	Windows DNS 服务器无法正确处理请求，造成了远程代码执行漏洞
	Microsoft Windows DNS Server	CVE-2018-8626	Windows DNS Server 堆溢出漏洞
EAP	EAP-PWD	CVE-2022-23304	EAP-PWD 中存在加密问题漏洞，攻击者可通过该漏洞发起侧通道攻击
FTP	Mobatek MobaXterm	CVE-2022-38337	Mobatek MobaXterm v22.1.2 前版本存在安全漏洞，可能会导致用户拒绝服务 (DoS)
	SolarWinds Serv-U FTP Server	CVE-2021-35211	SolarWinds Serv-U FTP Server 存在缓冲区错误漏洞，该漏洞可在目标系统上执行任意代码
	APK-Tools	CVE-2021-36159	FreeBSD Libfetch 跨界内存读
	FTP-Srv	CVE-2020-15152	FTP-Srv 允许PORT 命令请求服务器暗请求伪造漏洞
	Wing FTP Server	CVE-2020-8635	Wing FTP Server 中敏感的 Wing FTP 配置文件不安全的默认权限
	HAXX libcurl	CVE-2020-8285	恶意 FTP 服务器可以在使用 CURLOPT_CHUNK_BGN_FUNCTION 时触发堆栈溢出漏洞
HTTP	Apache Log4j	CVE-2021-45105	Apache Log4j 拒绝服务攻击漏洞
	XWiki Platform	CVE-2023-26477	XWiki Platform存在安全漏洞，该漏洞源于可以通过URL请求参数结合其他参数注入任意脚本宏
	Microsoft Windows	CVE-2022-21907	HTTP 协议堆栈远程代码执行漏洞
	Nagios Network Analyzer	CVE-2021-28925	Nagios Network_Analyzer SQL 命令中使用的特殊元素转义处理不恰当
	The ApacheOpen For Business Project	CVE-2021-26295	Apache OFBiz RMI 反序列化任意代码执行漏洞
	HTTP 协议栈	CVE-2021-31166	HTTP 协议堆栈远程代码执行漏洞
	F5 Networks	CVE-2021-22986	F5 BIG-IP/BIG-IQ Icontrol Rest 未授权远程代码执行漏洞
	Microsoft Exchange Server	CVE-2021-27065	Microsoft Exchange Server 允许任意设置文件名和路径导致文件写入漏洞
	Apache Tomcat	CVE-2020-1938	Tomcat AJP 文件读取与包含漏洞[Tomcat幽灵猫漏洞]
	F5 Networks	CVE-2020-5902	F5 BIG-IP 配置不当和缺乏身份验证导致远程代码执行漏洞
	D-Link	CVE-2019-16920	D-Link 命令注入漏洞
	Microsoft SharePoint	CVE-2019-0604	Microsoft SharePoint 输入验证不当导致远程代码执行漏洞
	Citrix Application Delivery Controller	CVE-2019-19781	Citrix ADC 允许未经身份验证的远程攻击者在目录遍历后在目标服务器上执行命令
	Drupal	CVE-2018-7600	Drupal 对表单请求内容未做严格过滤导致远程代码执行漏洞
	Apache Solr	CVE-2017-12629	Apache Solr XML 外部实体漏洞和远程命令执行漏洞
	Apache Tomcat	CVE-2017-12617	Apache Tomcat PUT 文件上传漏洞
	Apache Shiro	CVE-2016-4437	Apache Shiro 默认密钥致命令执行漏洞
HTTP2	VMware Spring Cloud Gateway	CVE-2022-22946	VMware Spring Cloud Gateway 存在信任管理问题漏洞，该漏洞允许本地用户绕过安全限制
	Apache Tomcat	CVE-2020-11996	Apache Tomcat 资源管理错误漏洞
	Apache Tomcat	CVE-2020-17527	Apache Tomcat 信息泄露漏洞
	Apache HTTP Server	CVE-2016-8740	Apache HTTP Server 拒绝服务漏洞
ICMP	Apple	CVE-2019-8605	IOS 内核任意地址读写漏洞
	Apple MacOS Sierra	CVE-2018-4407	Apple MacOS Sierra Kernel 代码执行漏洞
LDAP/HTTP	Apache Log4j	CVE-2021-44228	Apache Log4j loookup 功能输入验证不当导致远程代码执行漏洞

协 议	软 件	漏洞编号	漏洞描述
IIOP	IBM WebSphere Application Server	CVE-2020-4450	IBM WebSphere IIOP 协议的反序列化漏洞导致了远程代码执行漏洞
	Oracle WebLogic Server	CVE-2020-2551	Weblogic IIOP 协议反序列化漏洞
IMAP	Cyrus IMAP	CVE-2019-11356	Cyrus IMAP 缓冲区错误漏洞
	University of Washington IMAP Toolkit	CVE-2018-19518	University of Washington IMAP Toolkit imap_open 函数任意命令执行漏洞
	NEOJAPAN Denbun POP/Denbun IMAP	CVE-2018-0684	NEOJAPAN Denbun POP 及Denbun IMAP 之前版本中存在基于栈的缓冲区溢出漏洞
Kerberos	Microsoft Windows	CVE-2023-21817	Windows Kerberos 特权提升漏洞
	Microsoft Windows	CVE-2022-37966	Windows Kerberos RC4-HMAC 特权提升漏洞
	Microsoft Active Directory Domain Services	CVE-2021-42287	Microsoft Active Directory Domain Services允许潜在攻击者冒充域控制器的安全绕过漏洞
	Microsoft Active Directory Domain Services	CVE-2021-42278	Microsoft Active Directory Domain Services允许攻击者使用计算机账户SAMAccountName欺骗来冒充域控制器
	Microsoft Windows	CVE-2020-17049	Kerberos KDC 安全功能绕过漏洞
MariaDB	openSIS	CVE-2021-41678	SQL注入漏洞, 可利用该漏洞通过openSIS模块用户Staff .php..Staff[TITLE]参数发出SQL命令
	MariaDB	CVE-2020-7221	MariaDB mysql_install_db权限提升漏洞
	MongoDB Server	CVE-2019-2386	MongoDB Server 代码问题漏洞
	MongoDB Bson JavaScript module	CVE-2018-13863	MongoDB Bson JavaScript 模块安全漏洞
MS-LSAD	Samba	CVE-2016-2118	Samba MS-SAMR/MS-LSAD 中间人攻击漏洞[Badlock]
MySQL	MariaDB	CVE-2021-27928	MariaDB 操作系统命令注入漏洞
	Django	CVE-2020-7471	Django SQL在StringAgg(Delimiter) 的实现上注入漏洞
	Oracle MySQL/MariaDB/PerconaServe	CVE-2016-6664	Oracle MySQL/ MariaDB / PerconaDB 提权漏洞
	Oracle MySQL/MariaDB/PerconaServe	CVE-2016-6663	Oracle MySQL/ MariaDB / PerconaDB 提权/条件竞争漏洞
Netlogon	Microsoft Windows	CVE-2020-1472	Netlogon 中远程协议加密身份验证方案中的错误造成了特权提升漏洞
NTLM	Microsoft Windows	CVE-2023-21746	Windows NTLM 特权提升漏洞
	Microsoft Windows	CVE-2019-1040	Windows NTLM 篡改漏洞
	Microsoft Windows	CVE-2019-1338	Windows NTLM 安全功能绕过漏洞
	Adobe Acrobat/Adobe Reader	CVE-2018-4993	Adobe Acrobat/Reader NTLM SSO 哈希窃取漏洞
	Haxx Libcurl	CVE-2018-16890	Curl NTLM Type-2 堆缓冲区溢出漏洞
NTP	NTPsec	CVE-2021-22212	NTPsec 1.2.0存在安全漏洞, 该漏洞允许ntpKeygen生成密钥
	Rubetek Cameras	CVE-2020-25748	Rubetek 存在明文传输漏洞
	Juniper Networks Junos OS	CVE-2019-8936	Ntp NULL Pointer Dereference 拒绝服务漏洞
	Apache Web Server	CVE-2018-1232	NTP Ntpq/Ntpdc 栈缓冲区错误漏洞
	Meinberg IMS-LANTIME M3000	CVE-2016-3962	多款Meinberg产品基于栈的缓冲区溢出漏洞
TNS	Oracle Database Server	CVE-2021-35551	Oracle Database Server 输入验证错误漏洞
	Oracle Database Server	CVE-2019-2444	Oracle 组件存在本地提权效果的漏洞
	Oracle Database Server	CVE-2018-3110	Oracle Database Server Java VM 组件远程漏洞
POP3	Courier Mail Server	CVE-2021-38084	Courier Mail Server 注入漏洞
PostgreSQL	PostgreSQL	CVE-2022-21724	PostgreSQL JDBC 驱动远程代码执行漏洞
	PostgreSQL	CVE-2020-25695	PostgreSQL 12.5之前版本中存在SQL注入漏洞, 可以以超级用户的身份执行任意SQL函数
	PostgreSQL	CVE-2019-9193	PostgreSQL 任意代码执行漏洞
RDP	Microsoft Remote Desktop Services	CVE-2021-38666	允许未经认证的攻击者通过RDP连接目标设备并发送特殊构造的请求导致远程代码执行漏洞
	Microsoft Remote Desktop Services	CVE-2019-0708	CVE-2019-0708是与MS_T120 虚拟通道相关的内存破坏漏洞
	Microsoft Remote Desktop Services	CVE-2019-1181	让受影响的系统处理特制的 LNK 文件时会导致远程代码执行漏洞
RTSP	TP-Link TL-SC3130	CVE-2018-18428	TP-Link TL-SC3130 1.6.18版本中存在安全漏洞,攻击者可利用该漏洞泄露实时RTSP流

协 议	软 件	漏洞编号	漏洞描述
SMB	IBM AIX	CVE-2022-43381	IBM AIX存在拒绝服务漏洞, 未经授权的本地攻击者可利用该漏洞通过AIX SMB客户端实现拒绝服务
	Microsoft Server Message Block	CVE-2020-0796	Microsoft Windows SMBv3 输入验证错误漏洞[永恒之黑]
	Microsoft Windows	CVE-2017-0145	Windows SMBv1 Server 组件上存在远程代码执行漏洞
	Microsoft Windows	CVE-2017-0143	Windows SMB 大带分页池上存在缓冲区溢出[永恒之蓝]
SMTP	Opensmtpd	CVE-2020-8794	Opensmtpd mta_io 函数错误处理导致远程命令执行漏洞
	Opensmtpd	CVE-2020-7247	Opensmtpd smtp_mailaddr 函数无法正确处理用户输入导致远程代码执行漏洞
	Bitcoin Core	CVE-2019-11581	Atlassian Jira SMTP 模版注入远程代码执行漏洞
	开源邮件服务器Exim	CVE-2018-6789	Exim中SMTP 侦听器中的函数存在问题, 造成远程命令执行漏洞
SNMP	Airspan AirVelocity	CVE-2022-36310	速漏洞使具有SNMP写入能力的攻击者能够以ROOT权限执行任意命令
	CastleRock Computing SNMPc Online	CVE-2020-11557	SNMPc Online 不充分的凭证保护机制
	B&R Automation Runtime	CVE-2019-19108	SNMP 服务中的身份验证漏洞
	Zoom 5352	CVE-2018-20401	Zoom SNMP Request Credentials 凭证管理漏洞
	Cisco IOS/Cisco IOS XE	CVE-2017-6744	Cisco IOS/IOS XE SNMP系统中的缓冲区溢出漏洞
	Cisco IOS/Cisco IOS XE	CVE-2017-6742	Cisco IOS/IOS XE SNMP 服务缓冲区溢出漏洞
	Cisco IOS/Cisco IOS XE	CVE-2017-6738	Cisco IOS/IOS XE SNMP 内存破坏漏洞
	Cisco IOS/Cisco IOS XE	CVE-2017-6736	Cisco IOS/IOS XE SNMP 子系统缓冲区错误漏洞
	CloudView NMS	CVE-2016-5073	CloudView NMS SNMP 跨站脚本攻击
	Cisco Adaptive Security Appliance	CVE-2016-6366	Cisco Adaptive Security Appliance Software 堆栈缓冲区溢出漏洞
SQL Server	Microsoft SQL Server	CVE-2023-21713	Microsoft SQL Server 远程执行代码漏洞
SSH	Serv-U	CVE-2021-35211	SolarWinds Serv-U 不合法输入导致内存破坏漏洞
	OpenSSH	CVE-2021-28041	Openbsd Openssh ssh-agent 存在双重释放漏洞
	Libssh	CVE-2020-26301	SSH 存在操作系统命令注入漏洞, 导致Libssh2命令注入漏洞
	Libssh	CVE-2018-10933	Libssh 客户端允许没有身份验证的情况下创建通道, 导致了未授权访问漏洞
	OpenSSH	CVE-2016-6515	OpenSSH auth-passwd.c auth_password 拒绝服务漏洞
SSL	OpenSSL	CVE-2022-2068	错误地处理了c_rehash脚本导致本地攻击者可在运行c_rehash 时利用该漏洞执行任意命令
	OpenSSL	CVE-2021-3711	OpenSSL 缓冲区溢出漏洞
	F5 Networks	CVE-2016-9244	F5 BIG-IP设备存在TicketBleed 漏洞
	OpenSSL	CVE-2016-0800	Oracle Fujitsu M Server 加密问题漏洞
	OpenSSL	CVE-2014-0160	畸形的数据包导致的内存信息泄漏[HeartBleed心脏出血漏洞]
T3	Oracle Fusion Middleware	CVE-2022-21570	未经身份验证的攻击者可通过T3 IIOP协议网络, 导致Oracle Coherence挂起或频繁重复崩溃
	Oracle WebLogic Server	CVE-2020-2555	WebLogic ReflectionExtractor T3 反序列化远程命令执行漏洞
	Oracle WebLogic Server	CVE-2020-14825	Weblogic LockVersionExtractor T3 反序列化不可信数据远程代码执行漏洞
	Oracle Fusion Middleware	CVE-2020-2801	Oracle Fusion Middleware WebLogic Server Core 组件存在远程代码执行漏洞
	Oracle WebLogic Server	CVE-2020-2798	Oracle Weblogic Server 反序列化漏洞
	Oracle WebLogic Server	CVE-2020-14645	Weblogic UniversalExtractor T3 反序列化漏洞
	Oracle WebLogic Server	CVE-2018-3252	Oracle WebLogic Server 代码执行漏洞
	Oracle WebLogic Server	CVE-2018-3245	Oracle WebLogic Server WLS 反序列化漏洞
	Oracle WebLogic Server	CVE-2018-3191	Oracle WebLogic Server lookup 值可控导致远程代码执行漏洞
Telnet	FortiTester	CVE-2022-35846	漏洞源于 Telnet 端口中过度身份验证尝试的不当限制, 可被暴力破解
	Arch Linux	CVE-2021-22925	Telnet 存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
	TX9 Automatic Food Dispenser	CVE-2021-37555	TX9 Automatic Food Dispenser 信任管理问题漏洞
	Netkit-Telnet	CVE-2020-10188	Netkit Telnet 中没有边界检查允许远程执行任意代码
	Rubetek Cameras	CVE-2020-25749	Rubetek Rv-3406_Firmware 使用硬编码的凭证漏洞
	Rubetek Cameras	CVE-2020-25747	Rubetek 产品未授权访问漏洞
	Cisco IOS/Cisco IOS XE	CVE-2017-3881	多款Cisco产品IOS/IOS XE Software 输入验证错误漏洞
TLS	Microsoft Windows CryptoAPI	CVE-2020-0601	Microsoft Windows CryptoAPI 中加密证书的方法存在信任管理问题漏洞

科来官网：www.colasoft.com.cn 服务咨询电话：400 6869 069