【安全监测报告】奇安信 CERT 2020 年 9 月安全监测报告

截止 9 月 30 日，奇安信 CERT 共监测漏洞 74027 个，较上月新增漏洞 2514 个。其中有 969 条敏感信息 触发了人工研判标准 。经人工研判：本月值得重点关注的漏洞共 110 个，其中高风险漏洞共 38 个。

注：

1. 本月重要漏洞户口详情请点击“阅读原文”

2. 敏感漏洞触发条件由漏洞影响的产品、漏洞热度、可能的影响范围等多个维度综合判断

3. 人工研判流程包括对漏洞利用条件、影响范围、实际危害等多个方面的信息的综合研判

4. 针对高风险漏洞，奇安信 CERT 已于第一时间发布安全风险通告

5. 月度总舆论热度榜为奇安信 CERT 抓取到互联网上对该漏洞讨论次数汇总的榜单

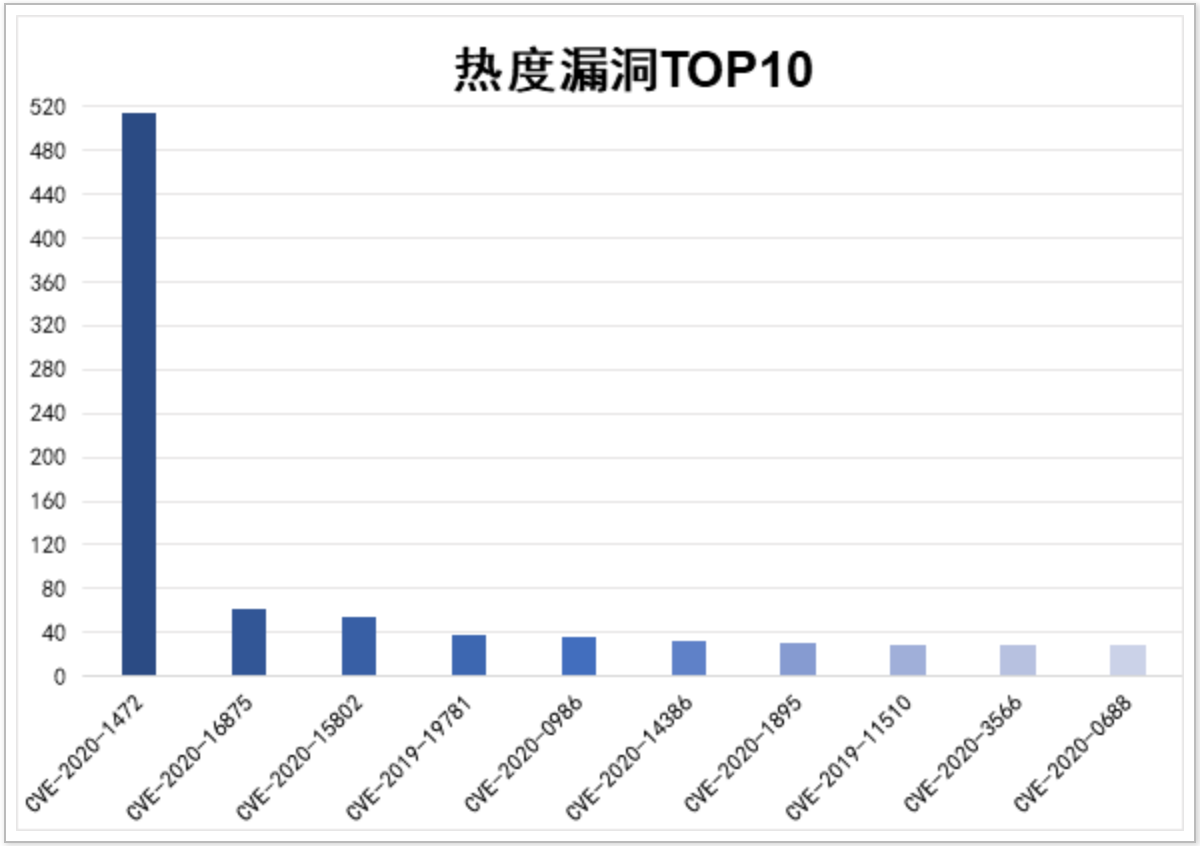
奇安信 CERT 9 月安全监测报告

月度总热度 Top10 漏洞概览

根据奇安信 CERT 的监测数据，在 2020 年 9 月份监测到的所有漏洞中，月度总舆论热度榜 TOP10 漏洞如下：

序号	漏洞热度	漏洞编号	影响产品	漏洞类型	CVSS 分数
1	515	CVE-2020-1472	NetLogon	权限提升	10
2	62	CVE-2020-16875	Microsoft Exchange	远程命令执行	7.2
3	54	CVE-2020-15802	Bluetooth	中间人攻击	5.9
4	38	CVE-2019-19781	Citrix ADC 和 Citrix 网关	远程代码执行	9.8

5	35	CVE-2020-0986	Windows splwow64	远程代码执行	7.8
6	32	CVE-2020-14386	Linux	权限提升	6.7
7	30	CVE-2020-1895	Instagram	远程代码执行	7.8
8	29	CVE-2019-11510	HTML5 Access	任意文件读取	10
9	29	CVE-2020-3566	Cisco IOS 和 Cisco IOS XR	拒绝服务	7.5
10	28	CVE-2020-0688	Exchange ECP	远程代码执行	8.8



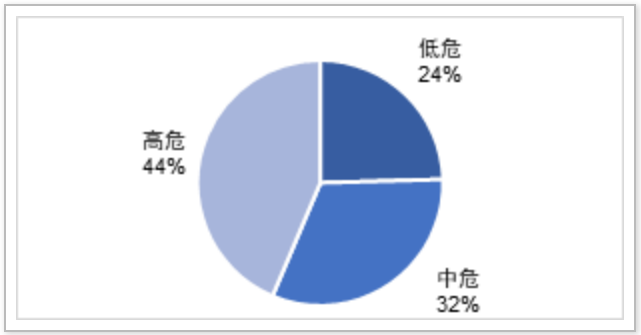
在 9 月月度总热度舆论榜前十的漏洞中，热度最高的漏洞为 NetLogon 特权提升漏洞（CVE-2020-1472），此漏洞允

许远程攻击者在不进行用户认证的情况下，尝试利用此漏洞。未经身份认证的攻击者可通过使用 Netlogon 远程协议（MS-NRPC）连接域控制器来利用此漏洞。成功利用此漏洞的攻击者可获得域管理员访问权限。

重点关注漏洞概览

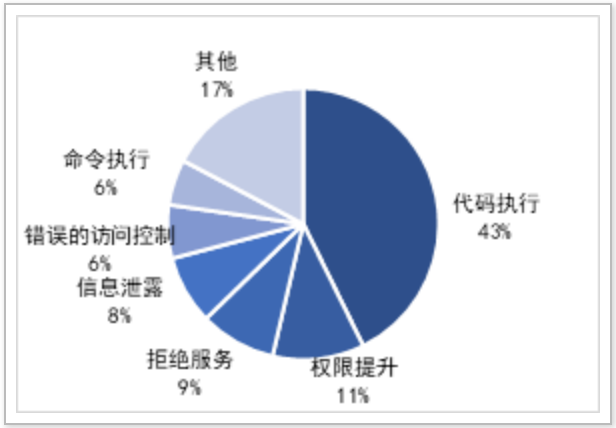
漏洞危害等级占比：

- 高危漏洞共 48 个，占比约为 44%
- 中危漏洞共 35 个，占比为为 32%
- 低危漏洞共 27 个，占比约为 24%



漏洞类型占比：

- 代码执行漏洞共 47 个，其占比约为 43%
- 权限提升漏洞共 12 个，其占比约为 11%
- 拒绝服务漏洞共 10 个，其占比约为 9%
- 信息泄露漏洞共 9 个，其占比各约为 8%



重点关注漏洞

漏洞编号	影响产品	危险等级	漏洞类型	触发方式
CVE-2020-1472	NetLogon	高危	权限提升	远程触发
CVE-2020-3566	Cisco IOS、Cisco IOS XR	中危	拒绝服务	远程触发
CVE-2020-3454	Cisco NX-OS	高危	权限提升	本地触发
CVE-2020-13946	Apache Cassandra	低危	中间人攻击	远程触发
CVE-2020-24584	Django 文件系统	低危	权限提升	本地触发

CVE-2020-14178	AtlassianJira Server	中危	信息泄露	远程触发
CVE-2020-3451	Cisco RV340	高危	命令执行	远程触发
CVE-2020-3495	Cisco Jabber	高危	代码执行	远程触发
CVE-2020-3545	Cisco FXOS	低危	远程代码执行	远程触发
CVE-2020-3530	Cisco IOS XR	中危	权限提升	本地触发
CVE-2020-12248	Foxit Reader PhantomPDF	高危	代码执行	本地触发
CVE-2020-13313	GitLab	高危	错误的访问控制	远程触发
CVE-2020-13311	GitLab Wiki	中危	拒绝服务	远程触发
CVE-2020-13316	GitLab	高危	身份认证绕过	远程触发
CVE-2019-0192	Apache Solr	高危	代码执行	远程触发
CVE-2020-13314	GitLab Omniauth Endpoint	低危	错误的访问控制	远程触发

CVE-2020-13315	GitLab	中危	拒绝服务	远程触发
CVE-2020-13317	GitLab	低危	错误的访问控制	远程触发
CVE-2020-11986	Apache NetBeans	中危	任意代码执行	远程触发
CVE-2020-0096	Android Framework	低危	权限提升	本地触发
CVE-2020-5855	BIG-IP Edge Client	低危	身份认证绕过	远程触发
CVE-2020-5896	BIG-IP Edge Client	低危	权限提升	远程触发
CVE-2019-20892	F5 SNMP	中危	拒绝服务	远程触发
用友 NC6.5 未授权反序列化漏洞	用友 NC6.5	高危	远程代码执行	远程触发
用友 NC6.5 SQL 注入漏洞	用友 NC6.5	高危	SQL 注入漏洞	远程触发
用友 NC6.5 XXE 漏洞	用友 NC6.5	高危	XML 外部实体注入 (XXE)	远程触发
CVE-2020-1200	Microsoft SharePoint	高危	代码执行	远程触发
CVE-2020-1210	Microsoft SharePoint	中危	代码执行	远程触发

CVE-2020-1452	Microsoft SharePoint	高危	代码执行	远程触发
CVE-2020-1453	Microsoft SharePoint	高危	代码执行	远程触发
CVE-2020-1576	Microsoft SharePoint	高危	代码执行	远程触发
CVE-2020-1595	Microsoft SharePoint	高危	代码执行	远程触发
CVE-2020-1460	Microsoft SharePoint	中危	代码执行	远程触发
CVE-2020-1319	Microsoft Windows Codecs Library	中危	代码执行	远程触发
CVE-2020-1129	Microsoft Windows Codecs Library	低危	代码执行	远程触发
CVE-2020-1285	Windows GDI+	中危	代码执行	远程触发
锐捷 EWEB 网关系统未授权任意命令执行漏洞	锐捷 EWEB 网管系统	高危	命令执行	远程触发
CVE-2020-1252	Windows	低危	代码执行	远程触发
CVE-2020-1508	Windows Media Audio Decoder	中危	代码执行	远程触发
CVE-2020-1593	Windows Media Audio Decoder	中危	代码执行	远程触发

CVE-2020-15903	nagios XI	中危	权限提升	未知
CVE-2020-0922	Microsoft COM for Windows	中危	代码执行	远程 触发
CVE-2020-15902	Nagios XI	中危	跨站脚本漏洞	远程 触发
CVE-2020-1894	WHATSAPP	高危	代码执行	远程 触发
CVE-2020-0878	Microsoft 浏览器	中危	代码执行	远程 触发
CVE-2019-8704	Keyboards	低危	信息泄露	本地 触发
CVE-2020-16862	Microsoft Dynamics　365 (on-premises)	高危	代码执行	远程 触发
CVE-2020-16857	Microsoft Dynamics 365 for Finance and Operations (on　-premises)	高危	代码执行	远程 触发
CVE-2020-0908	Windows	中危	代码执行	远程 触发
CVE-2020-1057	Scripting Engine	高危	代码执行	远程 触发
CVE-2020-1172	Scripting Engine	高危	代码执行	远程 触发
CVE-2020-0997	Windows Camera Codec Pack	高危	代码执行	远程 触发

CVE-2020-16874	Visual Studio	高危	代码执行	远程触发
CVE-2020-0664	Active Directory	高危	信息泄露	远程触发
CVE-2020-0856	Active Directory	高危	信息泄露	远程触发
CVE-2020-0941	Windows Win32k	中危	信息泄露	远程触发
CVE-2020-1152	Windows Win32k	高危	权限提升	远程触发
CVE-2020-1245	Windows Win32k	高危	权限提升	远程触发
CVE-2020-1308	DirectX	高危	权限提升	远程触发
CVE-2020-1115	Windows Common Log File System Driver	高危	权限提升	远程触发
CVE-2020-11998	Apache ActiveMQ　registry	低危	代码执行	远程触发
CVE-2020-7312	McAfee Agent (MA)	中危	任意代码执行	未知
CVE-2020-7315	McAfee Agent (MA)	中危	任意代码执行	未知
绿盟 UTS 综合威胁探针管理员任意登录漏洞	绿盟 UTS 综合威胁探针	高危	身份认证绕过	远程触发

深信服 EDR3.2.21 任意代码执行漏洞	深信服 EDR	高危	任意代码执行	远程触发
深信服 SSL VPN 远程命令执行漏洞	深信服 SSL VPN	高危	命令执行	远程触发
CVE-2020-11991	Apache Cocoon	高危	XML 外部实体注入	远程触发
用友 GRP-u8 命令执行	用友 GRP-u8	高危	命令执行	远程触发
泛微云桥任意文件读取	泛微云桥	中危	文件读取	远程触发
CVE-2020-1594	Microsoft Excel	中危	代码执行	远程触发
Nagios Xi 代码执行漏洞	Nagios Xi	中危	代码执行	远程触发
CVE-2020-13312	GitLab OAuth	低危	安全特性绕过	远程触发
CVE-2020-15148	Yii 2	中危	代码执行	远程触发
CVE-2020-24622	Nexus3	低危	信息泄露	远程触发
CVE-2020-2042	PAN-OS	低危	命令执行	远程触发
CVE-2020-16875	Microsoft Exchange	低危	命令执行	远程触发

CVE-2020-14181	Atlassian Jira Server 和 Data Center	中危	信息泄露	远程触发
CVE-2019-4279	IBM WebSphere Application Server ND	高危	代码执行	远程触发
CVE-2020-4450	WebSphere	高危	远程代码执行	远程触发
CVE-2020-4448	WebSphere	高危	代码执行	远程触发
CVE-2020-0618	微软 SQL Server Reporting Services	高危	代码执行	远程触发
CVE-2020-0264	Android libstagefright	高危	代码执行	远程触发
CVE-2020-14179	Atlassian Jira	中危	信息泄露	远程触发
CVE-2020-14177	Atlassian Jira	中危	拒绝服务	远程触发
CVE-2020-14180	Atlassian Jira	低危	信息泄露	远程触发
CVE-2020-4580	IBM DataPower Gateway	中危	拒绝服务	远程触发
CVE-2020-5421	Spring Framework RFD	低危	安全特性绕过	远程触发

CVE-2020-13948	Apache Superset	高危	代码执行	远程触发
CVE-2020-4643	WebSphere	高危	XML 外部实体注入	远程触发
CVE-2020-8147	npm utils-extend 模块	低危	远程代码执行	远程触发
CVE-2019-6713	ThinkCMF	低危	代码执行	远程触发
CVE-2020-2283	Jenkins Liquibase Runner 插件	低危	跨站脚本漏洞	远程触发
CVE-2020-2258	Jenkins CloudBees Plugin	低危	错误的访问控制	远程触发
CVE-2020-2267	Jenkins MongoDB Plugin	低危	错误的访问控制	远程触发
CVE-2020-3476	Cisco IOS-XE	中危	错误的访问控制	远程触发
CVE-2020-3417	Cisco IOS-XE	中危	代码执行	远程触发
CVE-2020-3403	Cisco IOS-XE	中危	命令执行	远程触发
CVE-2020-3404	Cisco IOS-XE	低危	身份认证绕过	远程触发
CVE-2020-5930	BIG-IP	低危	拒绝服务	远程触发

CVE-2020-12819	FortiGate SSL VPN	中危	拒绝服务	远程触发
CVE-2020-12820	FortiGate SSL VPN	低危	拒绝服务	远程触发
CVE-2020-12419	Mozilla Firefox	高危	代码执行	本地触发
CVE-2020-12420	Mozilla Firefox	高危	代码执行	本地触发
CVE-2020-3423	Cisco IOS XE	低危	权限提升	本地触发
用友 NC UploadController 未授权文件上传漏洞	用友 NC	高危	文件上传	远程触发
CVE-2020-5874	BIG-IP APM	中危	拒绝服务	远程触发
大汉网络政府建站系统存在通用 SQL 注入漏洞	大汉网络政府建站系统	高危	SQL 注入漏洞	远程触发
大汉网络邮箱系统通用密码重置漏洞	大汉网络邮箱系统	高危	安全特性绕过	远程触发
正方服务管理系统存在文件上传漏洞	正方服务管理系统	高危	文件上传	远程触发
CVE-2020-2279	Jenkins Script Security Plugin	中危	安全特性绕过	远程触发

高风险漏洞

漏洞编号	影响产品	漏洞类型	危险等级	触发方式	公开状态	详情链接
CVE-2020-1472	NetLogon	权限提升	高危	远程触发	漏洞细节、EXP已公开	点击查看
CVE-2020-4643	WebSphere	XML 外部实体注入	高危	远程触发	漏洞细节已公开	点击查看
CVE-2020-1200	Microsoft SharePoint	代码执行	高危	远程触发	未公开	点击查看
CVE-2020-1210	Microsoft SharePoint	代码执行	中危	远程触发	未公开	
CVE-2020-1452	Microsoft SharePoint	代码执行	高危	远程触发	未公开	

CVE-2020-1453	Microsoft SharePoint	代码执行	高危	远程触发	未公开
CVE-2020-1576	Microsoft SharePoint	代码执行	高危	远程触发	未公开
CVE-2020-1595	Microsoft SharePoint	代码执行	高危	远程触发	未公开
CVE-2020-1460	Microsoft SharePoint	代码执行	中危	远程触发	未公开
CVE-2020-1319	Microsoft Windows Codecs Library	代码执行	中危	远程触发	未公开
CVE-2020-1129	Microsoft Windows Codecs Library	代码执行	低危	远程触发	未公开

CVE-2020-1285	Windows GDI+	代码执行	中危	远程触发	未公开
CVE-2020-1252	Windows	代码执行	低危	远程触发	未公开
CVE-2020-1508	Windows Media Audio Decoder	代码执行	中危	远程触发	未公开
CVE-2020-1593	Windows Media Audio Decoder	代码执行	中危	远程触发	未公开
CVE-2020-0922	Microsoft COM for Windows	代码执行	中危	远程触发	未公开
CVE-2020-0878	Microsoft 浏览器	代码执行	中危	远程触发	未公开
CVE-2020-16862	Microsoft Dynamics 365 (on-premises)	代码执行	高危	远程触	未公开

			危	触发	
CVE-2020-16857	Microsoft Dynamics 365 for Finance and Operations (on-premises)	代码执行	高危	远程触发	未公开
CVE-2020-0908	Windows	代码执行	中危	远程触发	未公开
CVE-2020-16875	Microsoft Exchange	命令执行	低危	远程触发	未公开
CVE-2020-1057	Scripting Engine	代码执行	高危	远程触发	未公开
CVE-2020-1172	Scripting Engine	代码执行	高危	远程触发	未公开
CVE-2020-0997	Windows Camera Codec Pack	代码执行	高危	远程触发	未公开

CVE-2020-16874	Visual Studio	代码执行	高危	远程触发	未公开
CVE-2020-0664	Active Directory	信息泄露	高危	远程触发	未公开
CVE-2020-0856	Active Directory	信息泄露	高危	远程触发	未公开
CVE-2020-0941	Windows Win32k	信息泄露	中危	远程触发	未公开
CVE-2020-1152	Windows Win32k	权限提升	高危	远程触发	未公开
CVE-2020-1245	Windows Win32k	权限提升	高危	远程触发	未公开
CVE-2020-1308	DirectX	权限提升	高危	远程触发	未公开

			危	触发		
CVE-2020-1115	Windows Common Log File System Driver	权限提升	高危	远程触发	未公开	
锐捷 EWEB 网关系统未授权任意命令执行漏洞	锐捷 EWEB 网管系统	命令执行	高危	远程触发	未公开	暂无
深信服 EDR3.2.21 任意代码执行漏洞	深信服 EDR	任意代码执行	高危	远程触发	未公开	暂无
用友 GRP-u8 命令执行	用友 GRP-u8	命令执行	高危	远程触发	漏洞细节、POC 已公开	暂无
用友 NC6.5 SQL 注入漏洞	用友 NC6.5	SQL 注入漏洞	高危	远程触发	未公开	暂无
用友 NC6.5 XXE 漏洞	用友 NC6.5	XML 外部实体注入 (XXE)	高危	远程触发	未公开	暂无

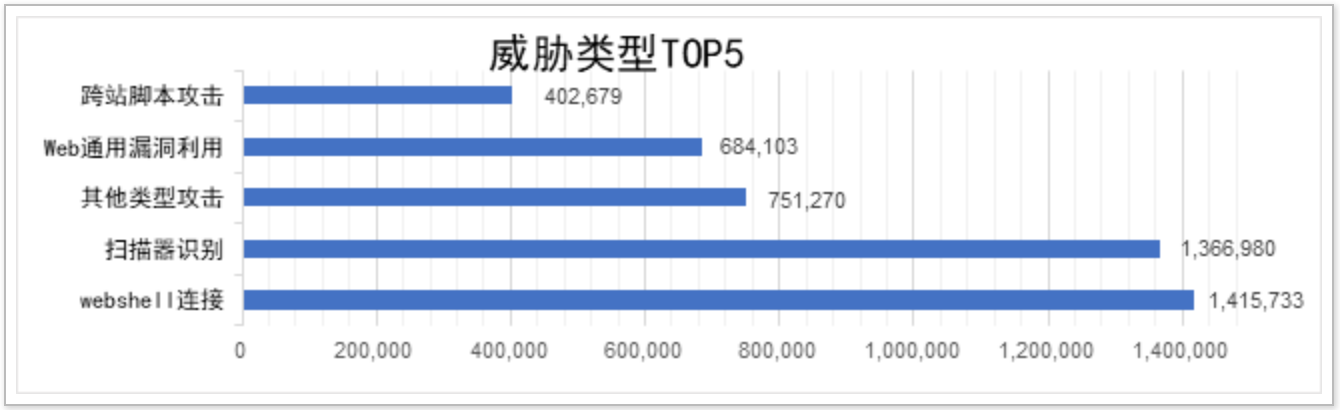
用友 NC6.5 未授权反序列化漏洞	用友 NC6.5	远程代码执行	高危	远程触发	未公开	暂无

威胁者信息

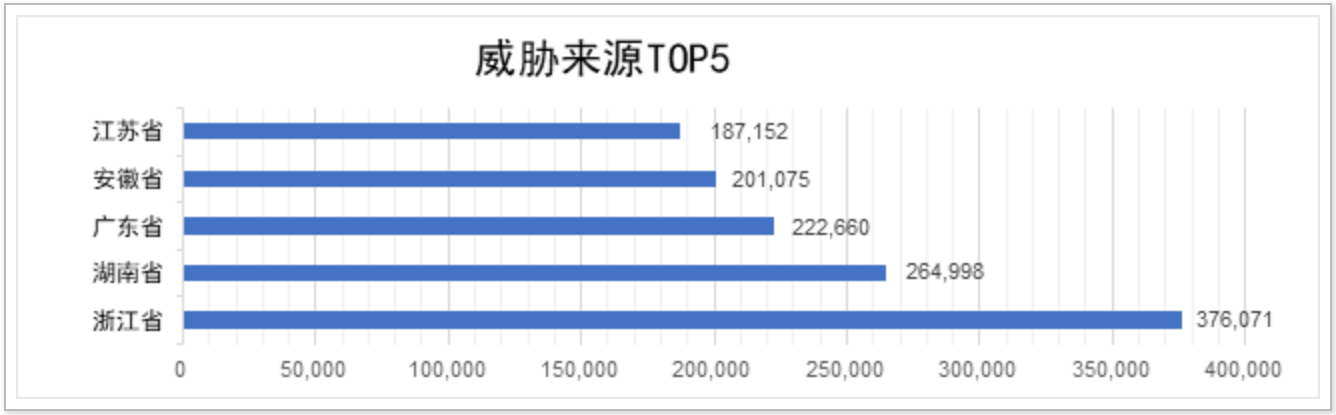
Web 漏洞被攻击者利用情况：

根据奇安信 CERT 白泽平台的攻击者画像数据，截止到 2020 年 9 月 30 日，奇安信 CERT 共识别出 1789839 个威胁者，通过 2079812 个 IP 地址发起攻击，其中共有 1895618 个 IP 为境内 IP，39827 个 IP 为来自境外。其中受威胁的网站数量为 54539，隐蔽链路为 95252 个。

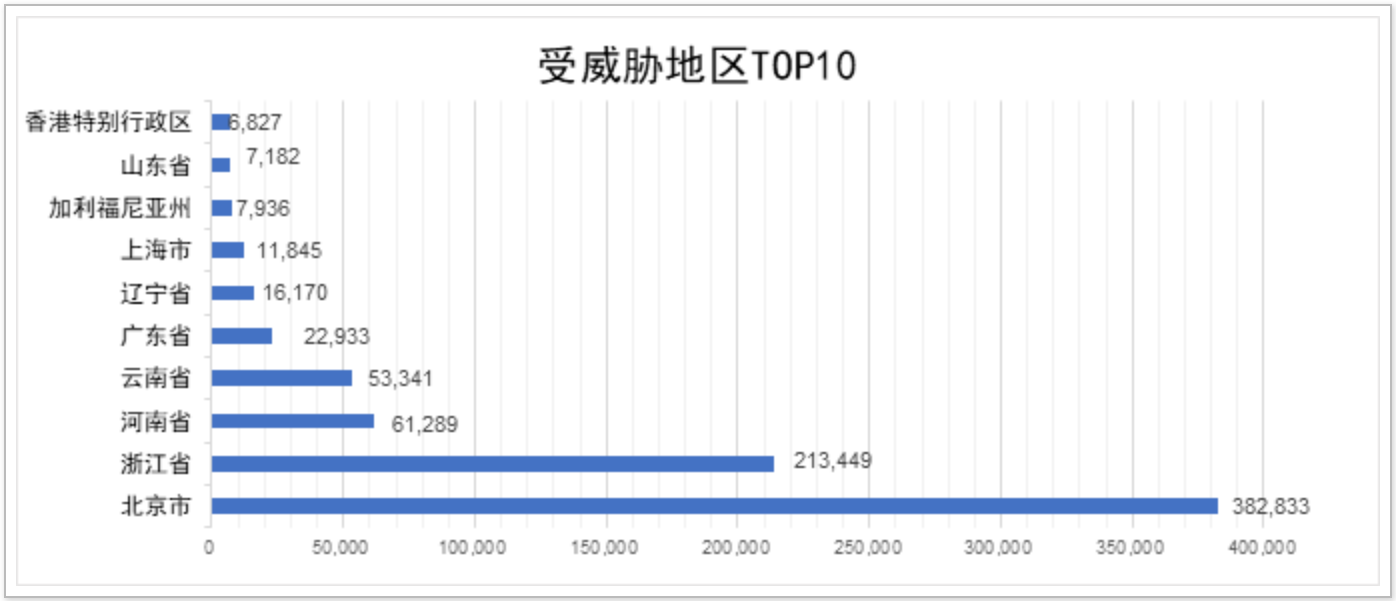
9 月威胁类型 TOP5 分别为：webshell 连接、Web 通用漏洞利用、扫描器识别、其他类型攻击、文件包含。



8 月威胁来源区域 TOP5 分别为浙江省、湖南省、广东省、安徽省、江苏省。



8 月受威胁地区 TOP10 为：北京市、浙江省、河南省、云南省、广东省、辽宁省、上海市、加利福尼亚州、山东省、香港特别行政区。



威胁者常用的威胁工具及手法如下：


Nsfocus Rsas
Grabber
Sangfor
Zgrab
WhatWeb
Nikto
Netsparker
M7lrv
Nmap
WebInspect
AWVS
WPscan
Yxlink_Scanner
Antsword
Nessus
SQLMap
APPscan
AppScan
Anonymous_Security
Burp
Paros
Xray
Hydra
MatriXay
Moresec
CnLuXun Scanner
HP
Metasploit
Dirbuster
Havij
Arachni


CNVD-2019-01092
Vul-2019-00124
CNVD-2018-24942
CVE-2019-11581
CNVD-2019-19299