警惕风险突出的 100 个高危漏洞

序号	漏洞名称	漏洞编号	漏洞危害
1	Apache Log4j2 远程代码执行漏洞	CVE-2021-44228	可直接远程控制相关服务器
2	Alibaba Nacos User-Agent 鉴权绕过漏洞	CVE-2021-29441	可直接绕过认证机制获取敏感数据
3	Oracle WebLogic Server 远程代码执行漏洞	CVE-2020-2884	可直接远程控制相关服务器
4	Apache Shiro 默认密钥致命令执行漏洞	CVE-2016-4437	可直接远程控制相关服务器
5	Spring Cloud Gateway spel 远程代码执行漏洞	CVE-2022-22947	可直接远程控制相关服务器
6	Atlassian Confluence 远程代码执行漏洞	CVE-2022-26134	可直接远程控制相关服务器
7	GitLab /uploads/user 远程命令执行漏洞	CVE-2021-22205	可直接远程控制相关服务器
8	Gitlabissuemarkdown 目录遍历漏洞	CVE-2020-10977	可以通过读取任意文件获取敏感信息
9	Apache Struts 代码执行漏洞	CVE-2023-50164	可直接远程控制相关服务器
10	redis 未授权访问漏洞	CNVD-2015-07557	可直接绕过认证机制获取敏感数据
11	Elasticsearch Kibana 命令注入漏洞	CVE-2019-7609	可直接远程控制相关服务器
12	Adobe ColdFusion 反序列化漏洞	CVE-2017-3066	可直接远程控制相关服务器
13	IIS6 WebDav 远程命令执行漏洞	CVE-2017-7269	可直接远程控制相关服务器
14	Apache ActiveMQ 远程代码执行漏洞	CVE-2023-46604	可直接远程控制相关服务器
15	Windows 打印后台处理程序远程执行代码漏洞	CVE-2021-34527	可直接远程控制相关服务器
16	F5 BIG-IP /tmui/login.jsp 远程代码执行漏洞	CVE-2020-5902	可直接远程控制相关服务器
17	Fortigate SSL VPN 路径遍历漏洞	CVE-2018-13379	可访问任意的文件获取敏感数据

18	Citrix ADC 远程代码执行漏洞	CVE-2019-19781	可直接远程控制相关服务器
19	Microsoft Exchange Server 认证绕过漏洞	CVE-2021-26857	可直接绕过认证机制获取敏感数据
20	Drupal geddon2 远程代码执行漏洞	CVE-2018-7600	可直接远程控制相关服务器
21	泛微 E-Office9 文件上传漏洞	CVE-2023-2523	可直接远程控制相关服务器
22	海康威视 IP Camera 身份认证绕过漏洞	CVE-2017-7921	可直接绕过认证机制获取敏感数据
23	畅捷通 T+ Upload.aspx 任意文件上传漏洞	CNVD-2022-60632	可直接远程控制相关服务器
24	禅道项目管理系统 misc-captcha-user.html 权限绕过&远程命令执行漏洞	CNVD-2023-02709	可直接远程控制相关服务器
25	宏景人力资源信息管理系统 /servlet/codesettree SQL 注入漏洞	CNVD-2023-08743	可执行任意 SQL 命令获取敏感数据
26	泛微 e-cology9 SQL 注入漏洞	CNVD-2023-12632	可执行任意 SQL 命令获取敏感数据
27	MinIO 未授权信息泄露漏洞	CVE-2023-28432	可直接访问未授权接口获取敏感信息
28	Elasticsearch Groovy Scripting Engine Sandbox 安全绕过漏洞	CVE-2015-1427	可直接远程控制相关服务器
29	WordPress WPLiveChat SupportPro 插件代码问题漏洞	CVE-2019-11185	可直接远程控制相关服务器
30	Apache ActiveMQ Jolokia 代码执行漏洞	CVE-2022-41678	可直接远程控制相关服务器
31	Atlassian Confluence Data Center&Server 权限提升漏洞	CVE-2023-22515	可导致低权限用户提升权限并执行管理操作
32	Memcached SASL 身份验证安全绕过漏洞	CVE-2013-7239	可直接绕过认证机制获取敏感数据
33	WordPress SnapCreek Duplicator 和 Duplicator Pro 路径遍历漏洞	CVE-2020-11738	可访问任意的文件获取敏感数据
34	QNAP Systems QTS 和 QuTS hero SQL 注入漏洞	CVE-2022-27596	可执行任意 SQL 命令获取敏感数据

序号	漏洞名称	漏洞编号	漏洞危害
35	GitLab CE and EE 不正确访问控制漏洞	CVE-2019-20148	可直接访问未授权接口获取敏感信息
36	Citrix ADC & Citrix Gateway 远程代码执行漏洞	CVE-2023-3519	可直接远程控制相关服务器
37	Apache RocketMQ NameServer 远程命令执行漏洞	CVE-2023-37582	可直接远程控制相关服务器
38	GitLab 信息泄露漏洞	CVE-2020-26413	可直接访问未授权接口获取敏感信息
39	Atlassian Confluence 远程代码执行漏洞	CVE-2023-22522	可直接远程控制相关服务器
40	ThinkPHP 信息泄露漏洞	CVE-2022-25481	可直接访问未授权接口获取敏感信息
41	泛微 E-Office /uploadify/uploadify.php 任意文件上传漏洞	CVE-2023-2648	可直接远程控制相关服务器
42	通达 OA delete_log.php 后台 SQL 注入漏洞	CVE-2023-4166	可执行任意 SQL 命令获取敏感数据
43	TeamCity 远程代码执行漏洞	CVE-2023-42793	可直接远程控制相关服务器
44	Zoho ManageEngine SAML 任意代码执行漏洞	CVE-2022-47966	可直接远程控制相关服务器
45	海康威视-综合安防管理平台 /center/api/files 任意文件上传漏洞	CNVD-2022-88855	可直接远程控制相关服务器
46	泛微 E-Office group_xml.php SQL 注入漏洞	CNVD-2022-43843	可执行任意 SQL 命令获取敏感数据
47	泛微 E-Office /iweboffice/officeserver.php 任意文件上传漏洞	CNVD-2022-43247	可直接远程控制相关服务器
48	Oracle Weblogic LockVersionExtractor T3 反序列化漏洞	CVE-2020-14825	可直接远程控制相关服务器
49	Apache Struts2 2.0.0～2.3.15 远程命令执行漏洞	CVE-2013-2251	可直接远程控制相关服务器
50	Oracle Weblogic RemoteConstructor IIOP T3 反序列化漏洞	CVE-2020-14644	可直接远程控制相关服务器

51	Apache Axis AdminService 远程代码执行漏洞	CVE-2019-0227	可直接远程控制相关服务器
52	Oracle WebLogic 反序列化漏洞	CVE-2020-2551	可直接远程控制相关服务器
53	多款 Red Hat 产品远程代码执行漏洞	CVE-2015-7501	可直接远程控制相关服务器
54	Oracle WebLogic Server WLS 组件远程代码执行漏洞	CVE-2018-3191	可直接远程控制相关服务器
55	Fastjson <1.2.83 远程代码执行漏洞	CVE-2022-25845	可直接远程控制相关服务器
56	Apache Solr 远程代码执行漏洞	CNVD-2023-27598	可直接远程控制相关服务器
57	Gitlab OmniAuth 账号劫持漏洞	CVE-2022-1162	可直接绕过认证机制获取敏感数据
58	WebLogic WLS 核心组件反序列化漏洞	CVE-2018-2628	可直接远程控制相关服务器
59	Oracle WebLogic Server WLS Core 组件安全漏洞	CVE-2018-2893	可直接远程控制相关服务器
60	JBoss Application Server JBossMQ JMS 反序列化漏洞	CVE-2017-7504	可直接远程控制相关服务器
61	Oracle WebLogic Console HTTP 协议远程代码执行漏洞	CVE-2020-14882	可直接远程控制相关服务器
62	Oracle Weblogic UniversalExtractor T3 反序列化漏洞	CVE-2020-14645	可直接远程控制相关服务器
63	Oracle WebLogic Server 安全漏洞	CVE-2020-14687	可直接远程控制相关服务器
64	Adobe ColdFusion 远程代码执行漏洞	CVE-2023-29300	可直接远程控制相关服务器
65	ThinkPHP lang 参数 远程命令执行漏洞	CVE-2022-47945	可直接远程控制相关服务器
66	Atlassian Confluence 远程代码执行漏洞	CVE-2021-26084	可直接远程控制相关服务器
67	大华智慧园区综合管理平台任意文件上传漏洞	CVE-2023-3836	可直接远程控制相关服务器
68	帆软报表 design_save_svg 任意文件覆盖漏洞	CNVD-2021-34467	可直接远程控制相关服务器

69	禅道项目管理系统 account 参数存在 SQL 注入漏洞	CNVD-2022-42853	可直接远程控制相关服务器
70	Oracle WebLogic Server wls9-async 组件反序列化漏洞	CVE-2019-2729	可直接远程控制相关服务器
71	Jenkins MetaClass 存在远程代码执行漏洞	CVE-2018-1000861	可直接远程控制相关服务器
72	华天动力 OA /ntkoupload.jsp 任意文件上传漏洞	CNVD-2022-54886	可直接远程控制相关服务器
73	F5 BIG-IP iControl REST device-stats 远程命令执行漏洞	CVE-2022-1388	可直接远程控制相关服务器
74	泛微 e-office UploadFile.php 文件上传漏洞	CNVD-2021-49104	可直接远程控制相关服务器
75	Atlassian Jira 授权问题漏洞	CVE-2022-0540	可直接绕过认证机制获取敏感数据
76	致远 OA /seeyon/htmlofficeservlet 路径任意文件写入漏洞	CNVD-2019-19299	可直接远程控制相关服务器
77	Spring Framework JDK >= 9 远程代码执行漏洞	CVE-2022-22965	可直接远程控制相关服务器
78	Laravel Framework Debug 远程代码执行漏洞	CVE-2021-3129	可直接远程控制相关服务器
79	GitLab 任意用户密码重置漏洞	CVE-2023-7028	可以通过重置用户密码接管代码管理平台，获取敏感信息
80	用友 NC BeanShell 存在命令执行漏洞	CNVD-2021-30167	可直接远程控制相关服务器
81	JeecgBoot JimuReport 模板注入导致命令执行漏洞	CVE-2023-4450	可直接远程控制相关服务器
82	Nacos Jraft Hessian 反序列漏洞	CNVD-2023-45001	可直接远程控制相关服务器
83	GeoServer 远程代码执行漏洞	CVE-2024-36401	可直接远程控制相关服务器

84	polkit（pkexec）权限提升漏洞	CVE-2021-4034	可导致低权限用户提升权限并执行管理操作
85	Metabase H2 远程代码执行漏洞	CVE-2023-38646	可直接远程控制相关服务器
86	TeamCity 认证绕过漏洞	CVE-2024-23917	可直接远程控制相关服务器
87	H2 Database 控制台远程代码执行漏洞	CVE-2021-42392	可直接远程控制相关服务器
88	Windows TCP/IP 远程代码执行漏洞	CVE-2024-38063	可直接远程控制相关服务器
89	CrushFTP 服务器端模板注入漏洞	CVE-2024-4040	可绕过身份验证获得管理访问权限，泄露敏感信息或执行代码
90	FortiGate SSL VPN 远程执行命令漏洞	CVE-2024-21762	可直接远程控制相关服务器
91	PHP CGI 参数注入远程执行命令漏洞	CVE-2024-4577	可直接远程控制相关服务器
92	Apache OFBiz 路径遍历代码执行漏洞	CVE-2024-36104	可直接远程控制相关服务器
93	Apache OfBiz 反序列化命令执行漏洞	CVE-2023-49070	可直接远程控制相关服务器
94	Rejetto HTTP File Server 远程代码执行漏洞	CVE-2024-23692	可直接远程控制相关服务器
95	Nexus Repository 3 目录遍历与文件读取漏洞	CVE-2024-4956	可访问任意的文件获取敏感数据
96	Palo Alto Networks PAN-OS GlobalProtect 命令注入漏洞	CVE-2024-3400	可直接远程控制相关服务器
97	泛微 E-Cology WorkflowServiceXml SQL 注入漏洞	QVD-2024-26136	可执行任意 SQL 命令获取敏感数据
98	Apache Solr Schema Designer 代码执行漏洞	CVE-2023-50292	可直接远程控制相关服务器
99	Apache Zeppelin shell 代码注入漏洞	CVE-2024-31861	可直接远程控制相关服务器
100	Zabbix Server Audit Log SQL 注入漏洞	CVE-2024-22120	可执行任意 SQL 命令获取敏感数据

安全防护提示

一、升级软件和更新补丁

1、跟踪软件安全更新：持续跟踪并评估软件供应商发布的安全更新信息。

2、持续扫描探测：利用自动化工具定期对系统进行扫描，识别缺失的安全补丁和更新。

3、更新管理流程规范化：建立规范的更新管理流程，确保所有安全更新和补丁的安装配置均经过测试和审批。

4、定期安全审计：加强对开源软件组件、通用软硬件风险排查，定期对系统数据库、中间件、网络设备等进行全面的安全审计，发现防护缺陷和逻辑漏洞。

二、强化边界防护

1、加固路由器与防火墙：明确网络连接点，严格限制访问控制列表，防止未授权访问。优化升级应用防火墙、流量检测等安全防护设备规则库。定期更新固件，禁用无关服务，减少漏洞攻击面。

2、强化代理与网关安全：优化代理和网关配置，过滤恶意流量，阻挡潜在漏洞利用的威胁。使用高级代理检查加密流量，配置邮件网关过滤垃圾邮件和恶意附件。

3、更新威胁情报：定期更新防火墙和网关设备的威胁情报库，保持防护有效性，及时应对新型漏洞攻击手法。

4、日志监控与审计：集中监控和分析边界设备日志，及时发现攻击行为。利用安全信息与事件管理系统整合日志，识别异常并自动响应。

三、监测与加固内网

1、持续漏洞扫描与评估：部署漏洞扫描工具，定期扫描内网关键系统，识别并优先修复高危漏洞。

2、网络流量监控与分析：实时监控外联访问行为，检测异常行为，防止被植入木马后门。

3、用户行为监控：监控用户在内网的操作行为，识别异常活动和潜在的风险行为，定时分析用户行为模式，及时发现并处理不符合安全策略的行为。

4、内网资产管理：维护内网资产清单，确保设备和应用受控，减少安全风险。

5、系统加固与配置优化：调整系统配置，实施访问控制和最小权限原则。定期进行系统基线检查，确保配置符合安全标准。

四、加强终端防护

1、终端安全管理：在终端设备上安装安全检测工具，实时监控和处理潜在威胁。确保漏洞库及时更新，并严格执行保护策略，防止设备受到攻击。

2、数据加密与防泄漏：对敏感数据进行全面加密，防止在设备丢失或被盗时数据泄露。限制数据存放位置，避免在网站目录下直接存储备份文件或包含敏感信息的文档。

3、用户行为控制：限制风险操作，防止安装未授权的软件和访问可疑网站。实施防范社会工程攻击的措施，如识别虚假信息和防止信息泄露。

国家网络安全通报中心