**2024年2月23日入侵检测特征库升级公告**

IPS特征库版本号:IPS-20240223-1.1.1.30

发表日期：2024-2-23

**目前入侵检测库规则总数量为：9855条**

|  |  |  |
| --- | --- | --- |
| **漏洞(编号/类型)/病毒名** | **特征摘要** | **特征说明** |
| 暂无 | 万户ezOffice upload.jsp接口jsp文件上传尝试 |  |
| 暂无 | 海康威视综合安防管理平台report接口jsp文件上传尝试 |  |
| 暂无 | 海康威视综合安防管理平台files接口jsp文件上传尝试 |  |
| 暂无 | Hytec Inter HWL-2511-SS popen.cgi接口远程命令注入尝试 |  |
| 暂无 | 绿盟NF下一代防火墙php文件上传尝试 |  |
| CVE-2023-41265 | Qlik Sense HTTP请求隧道利用尝试（CVE-2023-41265） |  |
| CVE-2023-41266 | Qlik Sense路径遍历尝试（CVE-2023-41266） |  |
| CVE-2023-43177 | CrushFTP远程代码执行尝试（CVE-2023-43177） |  |
| CVE-2023-6038 | H2O任意文件读取尝试（CVE-2023-6038） |  |
| CVE-2023-6021 | Ray日志接口任意文件读取尝试（CVE-2023-6021） |  |
| CVE-2023-6020 | Ray /static/接口任意文件读取尝试（CVE-2023-6020） |  |
| CVE-2023-46604 | Apache ActiveMQ远程代码执行尝试（CVE-2023-46604） |  |
| CVE-2023-49796/CVE-2023-50731 | MindsDB任意文件写入尝试（CVE-2023-49796/CVE-2023-50731） |  |
| 暂无 | 用友NC6.5 grouptemplet接口jsp文件上传尝试 |  |
| 暂无 | 用友NC Cloud accept.jsp接口jsp文件上传尝试 |  |
| CVE-2023-28662 | WordPress插件 Gift Cards SQL注入尝试（CVE-2023-28662） |  |
| CVE-2023-27637/CVE-2023-27638 | PrestaShop SQL注入尝试（CVE-2023-27637/CVE-2023-27638） |  |
| CVE-2023-25207 | PrestaShop SQL注入尝试（CVE-2023-25207） |  |
| CVE-2022-30452 | Shopwind SQL注入尝试（CVE-2022-30452） |  |
| CVE-2021-36440/CVE-2022-1034 | ShowDoc v2.9.5文件上传尝试（CVE-2021-36440/CVE-2022-1034） |  |
| CVE-2020-23978 | Soluzione Globale电子商务cms SQL注入尝试（CVE-2020-23978） |  |
| CVE-2020-9269 | SOPlanning 1.45 SQL注入尝试（CVE-2020-9269） |  |
| CVE-2022-3118 | Sourcecodehero ERP系统SQL注入尝试（CVE-2022-3118） |  |
| CVE-2017-11444 | Subrion CMS SQL注入尝试（CVE-2017-11444） |  |
| CVE-2023-0244 | TuziCMS SQL注入尝试（CVE-2023-0244） |  |
| CVE-2022-26301 | TuziCMS SQL注入尝试（CVE-2022-26301） |  |
| CVE-2021-44349 | TuziCMS SQL注入尝试（CVE-2021-44349） |  |
| CVE-2021-44348 | TuziCMS SQL注入尝试（CVE-2021-44348） |  |
| CVE-2021-44347 | TuziCMS SQL注入尝试（CVE-2021-44347） |  |
| CVE-2019-16644 | TuziCMS SQL注入尝试（CVE-2019-16644） |  |
| CVE-2019-16642 | TuziCMS SQL注入尝试（CVE-2019-16642） |  |
| CVE-2019-12251 | UCMS SQL注入尝试（CVE-2019-12251） |  |
| CVE-2021-26473 | Vembu未经身份验证的文件上传尝试（CVE-2021-26473） |  |
| CVE-2021-26471 | Vembu未经验证的远程代码执行尝试（CVE-2021-26471） |  |
| CVE-2019-9859 | Vesta控制面板远程代码执行尝试（CVE-2019-9859） |  |
| CVE-2015-4117 | Vesta控制面板远程代码执行尝试（CVE-2015-4117） |  |
| CVE-2022-28060 | VictorCMS SQL注入尝试（CVE-2022-28060） |  |
| CVE-2020-35597 | VictorCMS SQL注入尝试（CVE-2020-35597） |  |
| CVE-2020-23945 | VictorCMS SQL注入尝试（CVE-2020-23945） |  |
| CVE-2017-15992 | Website Broker脚本SQL注入尝试（CVE-2017-15992） |  |
| CVE-2021-25899 | Void Aural Rec Monitor SQL注入尝试（CVE-2021-25899） |  |
| CVE-2015-5452 | Watchguard XCS SQL注入尝试（CVE-2015-5452） |  |
| CVE-2015-9462 | awesome-filterable-portfolio SQL注入尝试（CVE-2015-9462） |  |
| CVE-2015-9461 | awesome-filterable-portfolio SQL注入尝试（CVE-2015-9461） |  |
| CVE-2021-24137 | Blog2Social WordPress插件SQL注入尝试（CVE-2021-24137） |  |
| CVE-2015-9467 | broken-link-manager插件SQL注入尝试（CVE-2015-9467） |  |
| CVE-2015-9467 | broken-link-manager插件SQL注入尝试（CVE-2015-9467） |  |
| 哥斯拉 | 哥斯拉php webshell连接尝试 |  |
| 菜刀 | 菜刀aspx webshell连接尝试 |  |
| 暂无 | DS\_Store查询尝试 |  |
| 暂无 | Git存储库查找尝试 |  |
| 菜刀 | 菜刀php webshell连接尝试 |  |
| 蚁剑 | 蚁剑php webshell通信尝试 |  |
| 蚁剑 | 蚁剑php webshell通信尝试 |  |
| 冰蝎 | 冰蝎 v3 CnC（默认密码）-入站尝试 |  |
| 冰蝎 | 冰蝎 Webshell asp上传尝试 |  |
| 冰蝎 | 冰蝎 Webshell jsp上传尝试 |  |
| 冰蝎 | 冰蝎 Webshell jsp上传尝试 |  |
| 暂无 | Webshell php上传尝试 |  |
| 暂无 | Webshell php上传尝试 |  |
| Altman | Altman Webshell asp上传尝试 |  |
| 暂无 | 经过编码的Webshell asp上传尝试 |  |
| 暂无 | O2OA open接口任意文件读取尝试 |  |
| CNVD-2023-12632 | 泛微OA E-Cology browser.jsp接口SQL注入尝试（CNVD-2023-12632） |  |
| CVE-2023-25690 | Apache HTTP服务器私自请求尝试（CVE-2023-25690） |  |
| CVE-2023-2825 | GitLab CE/EE目录遍历尝试（CVE-2023-2825） |  |
| CVE-2022-0847 | Linux Kernel Dirty Pipe权限提升尝试（CVE-2022-0847） |  |
| CVE-2022-0847 | Linux Kernel Dirty Pipe权限提升尝试（CVE-2022-0847） |  |
| CVE-2023-21839 | Oracle WebLogic Server未经身份验证的RMI代码执行尝试（CVE-2023-21839） |  |
| CVE-2023-21839 | Oracle WebLogic Server未经身份验证的RMI代码执行尝试（CVE-2023-21839） |  |
| CVE-2022-25845 | Fastjson反序列化RCE尝试（CVE-2022-25845） |  |
| CVE-2023-34928 | H3C Magic B1STV100R012堆栈溢出尝试（CVE-2023-34928） |  |
| CNVD-2022-86535 | ThinkPHP RCE尝试（CNVD-2022-86535） |  |
| CobaltSteke | CobaltSteke http信标 - 心跳（出站） |  |
| CobaltSteke | CobaltSteke http信标 - 数据回传（出站） |  |
| CobaltSteke | CobaltSteke https信标 - 客户端hello消息（出站） |  |
| CobaltSteke | CobaltStrake dns信标 - c2响应（入站） |  |
| CobaltSteke | CobaltStrake dns信标 - c2响应（入站） |  |
| 暂无 | D-Link DAR-8000和百卓Smart importhtml.php远程命令执行尝试 |  |
| 暂无 | 海康威视视频编码设备网关任意文件读取尝试 |  |
| 暂无 | MagicFlow防火墙网关main.xp任意文件读取尝试 |  |
| 暂无 | Selea OCR-ANPR摄像机get\_file.php任意文件读取尝试 |  |
| 暂无 | Selea OCR-ANPR相机任意文件读取尝试 |  |
| 暂无 | Teleport堡垒机get-file任意文件读取尝试 |  |
| 暂无 | 腾达 11N无线路由器登录绕过尝试 |  |
| CVE-219-16313 | 蜂网互联企业级路由器v4.31用户名和密码泄露尝试（CVE-2019-16313） |  |
| CVE-2021-28152 | 宏电H8922 Telnet后门访问尝试（CVE-2021-28152） |  |
| CVE-2021-28152 | 宏电H8922 Telnet后门访问尝试（CVE-2021-28152） |  |
| CVE-2021-28150 | 宏电H8922用户名和密码泄露尝试（CVE-2021-28150） |  |
| 暂无 | 锐捷Smartweb管理系统用户名和密码泄露尝试 |  |
| 暂无 | AspCMS commentList.asp SQL注入尝试 |  |
| CVE-219-16131 | OKLite插件安装php文件上传尝试（CVE-2019-16131） |  |
| 暂无 | OpenSNS CurlModel.class.php SSRF尝试 |  |
| 暂无 | ".env"文件访问尝试 |  |
| CVE-2017-16894 | Laravel .env配置文件信息泄露（CVE-2017-16894） |  |
| CVE-2021-26885 | Microsoft Exchange SSRF攻击尝试（CVE-2021-26885） |  |
| CVE-2021-37580 | Apache ShenYu DashboardUser用户名和密码泄露（CVE-2021-37580） |  |
| CVE-2022-39952 | Fortinet FortiNAC任意文件写入尝试（CVE-2022-39952） |  |
| CVE-2023-21932 | Oracle Opera RCE尝试（CVE-2023-21932） |  |
| CVE-2023-29489 | cPanel XSS漏洞攻击尝试（CVE-2023-29489） |  |
| 冰蝎 | 冰蝎4.0webshell管理工具特征 |  |
| 冰蝎 | 冰蝎4.0webshell管理工具特征 |  |
| 冰蝎 | 冰蝎4.0webshell管理工具特征 |  |
| 冰蝎 | 冰蝎4.0webshell管理工具特征 |  |
| 冰蝎 | 冰蝎4.0webshell管理工具特征 |  |
| 冰蝎 | 冰蝎4.0webshell管理工具特征 |  |
| 冰蝎 | 冰蝎4.0webshell管理工具特征 |  |
| 冰蝎 | 冰蝎4.0webshell管理工具特征 |  |
| 冰蝎 | 冰蝎4.0webshell管理工具特征 |  |
| 暂无 | 检测到ASP上传webshell |  |
| 暂无 | webshell上传JSP尝试 |  |
| 暂无 | webshell上传PHP尝试 |  |
| 暂无 | webshell上传ASPX尝试 |  |
| CVE-2015-1830 | Apache ActiveMQ目录遍历尝试(CVE-2015-1830) |  |
| CVE-2018-6892 | CloudMe Sync客户端堆栈缓冲区溢出尝试(CVE-2018-6892) |  |
| CVE-2018-6892 | CloudMe Sync客户端堆栈缓冲区溢出尝试(CVE-2018-6892) |  |
| CVE-2018-6892 | CloudMe Sync客户端堆栈缓冲区溢出尝试(CVE-2018-6892) |  |
| CVE-2020-25687 | Dnsmasq extract\_name缓冲区溢出尝试(CVE-2020-25687) |  |
| CVE-2020-25681 | Dnsmasq sort\_rrset缓冲区溢出尝试(CVE-2020-25681) |  |
| CVE-2020-25683 | Dnsmasq PX响应堆溢出尝试(CVE-2020-25683) |  |
| CVE-2020-25682 | Dnsmasq PX extract\_name缓冲区溢出尝试(CVE-2020-25682) |  |
| CVE-2023-25136 | OpenSSH已弃用的WinSCP版本攻击尝试（CVE-2023-25136） |  |
| CVE-2023-25136 | OpenSSH弃用的PuTTY版本攻击尝试（CVE-2023-25136） |  |
| CVE-2022-27926 | Zimbra Collaboration Suite跨站脚本漏洞(CVE-2022-27926) |  |
| CVE-2022-27926 | Zimbra Collaboration Suite跨站脚本漏洞(CVE-2022-27926) |  |
| CVE-2022-32300 | YouDianCMS SQL注入尝试（CVE-2022-32300） |  |
| CVE-2021-32682 | ELFINDER ZIP 命令注入尝试（CVE-2021-32682） |  |
| CVE-2020-26124 | OpenMediaVault rpc.php经过身份验证的php代码注入尝试（CVE-2020-26124） |  |
| CVE-2022-22980 | Spring Data MongoDB SpEL Expression注入尝试（CVE-2022-22980） |  |
| CVE-2019-18873 | FUDForum 3.0.9-远程代码执行尝试（CVE-2019-18873） |  |
| 暂无 | PHP Melody v3.0 SQL注入攻击 |  |
| CVE-2021-30461 | VoIPmonitor 远程命令执行尝试（CVE-2021-30461） |  |
| CVE-2020-18716 | Rockoa v1.8.7 SQL注入尝试（CVE-2020-18716） |  |
| CVE-2019-9846 | Rockoa v1.8.7敏感信息尝试（CVE-2019-9846） |  |
| CVE-2021-44427 | Rosario Student Information System SQL注入尝试（CVE-2021-44427） |  |
| CVE-2020-12640 | Roxy WI远程代码执行尝试（CVE-2020-12640） |  |
| CVE-2022-43288 | Rukovoditel-3.2.1 SQL注入尝试（CVE-2022-43288） |  |
| CVE-2022-31137 | Roxy-WI未经身份验证的命令注入尝试(CVE-2022-31137) |  |
| CVE-2022-31137 | Roxy-WI未经身份验证的命令注入尝试(CVE-2022-31137) |  |
| CVE-2022-31137 | Roxy-WI未经身份验证的命令注入尝试(CVE-2022-31137) |  |
| CVE-2022-31137 | Roxy-WI未经身份验证的命令注入尝试(CVE-2022-31137) |  |
| CVE-2022-37061 | FLIR AX8 Camera命令注入尝试(CVE-2022-37061) |  |
| CVE-2022-37061 | FLIR AX8 Camera命令注入尝试(CVE-2022-37061) |  |
| CVE-2021-41674 | E-Negosyo-System SQL注入尝试(CVE-2021-41674) |  |
| CVE-2023-25194 | Apache Druid远程代码执行尝试（CVE-2023-25194） |  |
| 暂无 | Apache Hadoop YARN ResourceManager任意命令执行尝试 |  |
| CVE-2023-32071 | XWiki平台xss尝试(CVE-2023-32071) |  |
| CVE-2021-31805 | Apache Struts OGNL 沙箱绕过尝试（CVE-2021-31805） |  |
| CVE-2021-41674 | E-Negosyo-System SQL注入尝试（CVE-2021-41674） |  |