# Vite 任意文件读取漏洞 (CVE-2025-30208)

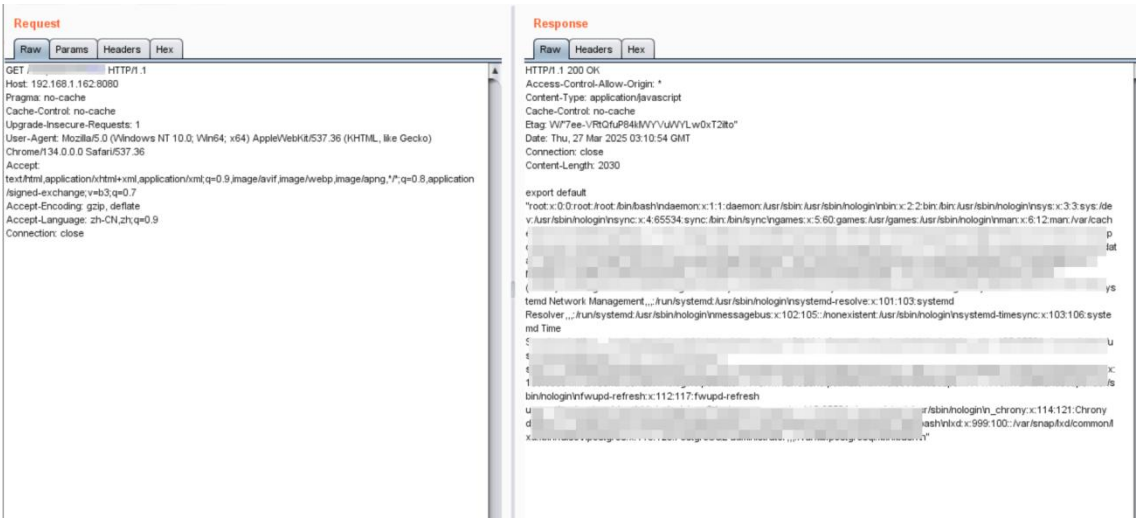
| | | | |
|---|---|---|---|
| ■ **通告编号** | **NS-2025-0017-1** | ■ 发布日期 | **2025-03-31** |
| ■ **漏洞危害** | **攻击者利用此漏洞，可实现任意文件读取。** | | |
| ■ **TAG** | Vite、任意文件读取、CVE-2025-30208 | | |

# 一. 漏洞概述

近日，绿盟科技 CERT 监测到 Vite 发布安全公告，修复了 Vite 任意文件读取漏洞(CVE-2025-30208)；由于 Vite 开发服务器在处理 URL 请求时未对路径进行严格校验，未经身份验证的攻击者可以通过构造特殊的 URL 绕过路径访问限制，从而读取目标服务器上的任意文件。目前漏洞细节与 PoC 已公开，请相关用户尽快采取措施进行防护。

Vite 是一个现代化的前端开发与构建工具，提供极速的开发服务器启动速度和高效的热更新机制，支持多框架开发，如 Vue、React 等。因其出色的性能和丰富的插件生态，成为前端开发领域的热门选择。

绿盟科技已成功复现此漏洞：




参考链接：

https://github.com/vitejs/vite/security/advisories/GHSA-x574-m823-4x7w

# 二. 影响范围

**受影响版本**

- 6.2.0 <= Vite <= 6.2.2

- 6.1.0 <= Vite <= 6.1.1
- 6.0.0 <= Vite <= 6.0.11
- 5.0.0 <= Vite <= 5.4.14
- Vite <= 4.5.9

注：影响将 Vite 开发服务器暴露到网络（启用--host 或配置 server.host）的应用。

**不受影响版本**

- Vite >= 6.2.3
- 6.1.2 <= Vite < 6.2.0
- 6.0.12 <= Vite < 6.1.0
- 5.4.15 <= Vite < 6.0.0
- 4.5.10 <= Vite < 5.0.0

# 三. 漏洞检测

## 3.1 人工检测

相关用户可通过查看当前 Vite 版本是否在受影响范围，对当前服务是否受此漏洞影响进行排查。

通过 npm 全局安装的可使用下列命令进行查看：

```
D:\>npm list -g vite
C:\Users\nsfocus\AppData\Roaming\npm
`-- vite@6.2.3
```

也可在终端命令行直接运行 vite -v 命令查看：

```
C:\Users\nsfocus>vite -v
vite/6.2.3 win32-x64 node-v18.19.0
```

## 3.2 工具检测

绿盟科技自动化渗透测试工具（EZ）已支持 Vite 的指纹识别和 CVE-2025-30208 漏洞风险检测（注：企业版请联系绿盟销售人员获取）。

用户可使用下列命令进行漏洞检测：

```
./ez webscan --pocs vite -u  https:192.168.1.41:443/
```


工具下载链接：https://github.com/m-sec-org/EZ/releases

新用户请注册 M-SEC 社区（https://msec.nsfocus.com）申请证书进行使用：


注：社区版本将于近期发布上述功能

## 3.3 产品检测

绿盟科技远程安全评估系统（RSAS）与 WEB 应用漏洞扫描系统(WVSS)已具备对此次漏洞的扫描与检测能力，请有部署以上设备的用户升级至最新版本。

| | 升级包版本号 | 升级包下载链接 |
|---|---|---|
| **RSAS V6 系统插件包** | V6.0R02F01.3909 | https://update.nsfocus.com/update/listRsasDetail/v/vulsys |
| **RSAS V6 Web 插件包** | V6.0R02F00.3707 | https://update.nsfocus.com/update/listRsasDetail/v/vulweb |

| | | |
|---|---|---|
| **WVSS V6 插件升级包** | V6.0R03F00.350 | https://update.nsfocus.com/update/listWvssDetail/v/6/t/plg |

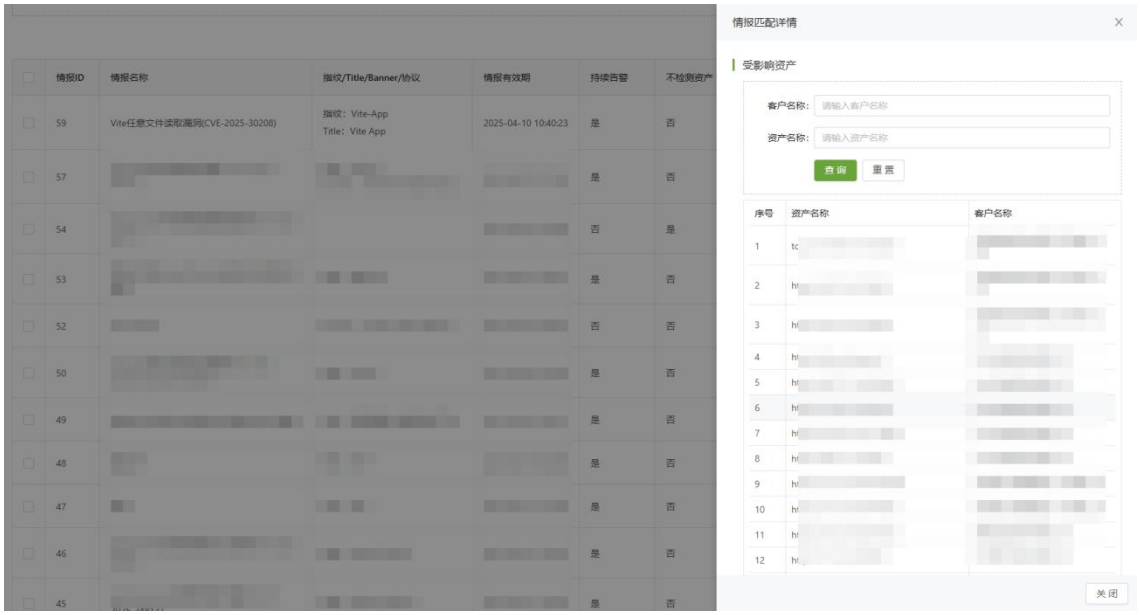
关于 RSAS 的升级配置指导，请参考如下链接：

https://mp.weixin.qq.com/s/SgOaCZeKrNn-4uR8Yj_C3Q

# 四. 暴露面风险排查

## 4.1 云端检测

绿盟科技外部攻击面管理服务（EASM）支持 CVE-2025-30208 漏洞风险的互联网资产排查，目前已帮助服务客户群体完成了暴露面排查与风险验证，在威胁发生前及时进行漏洞预警与闭环处置。



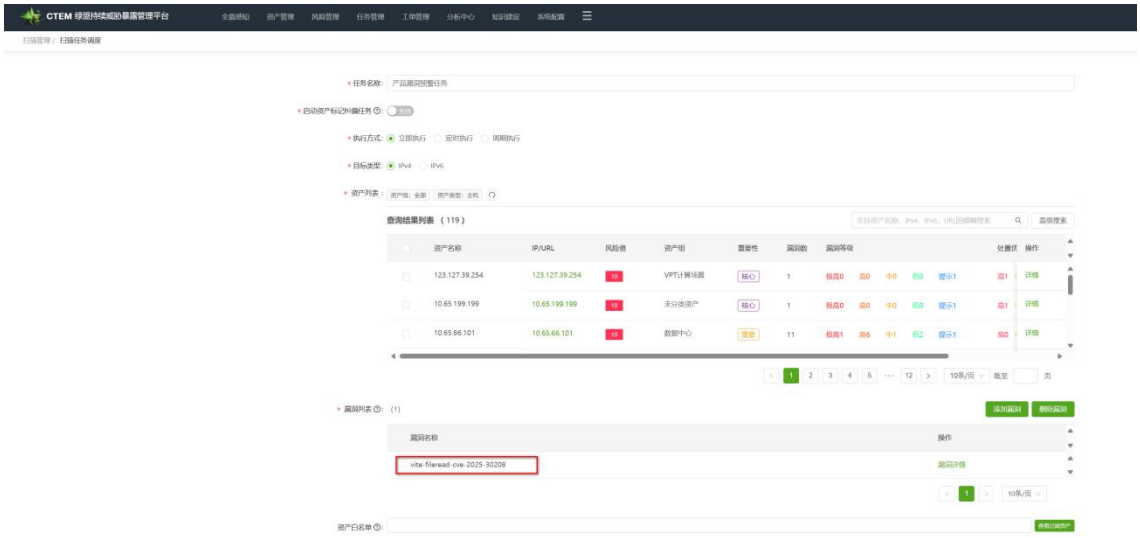

感兴趣的客户可通过联系绿盟当地区域同事或发送邮件至 rs@nsfocus.com 安排详细的咨询交流。


## 4.2 本地排查

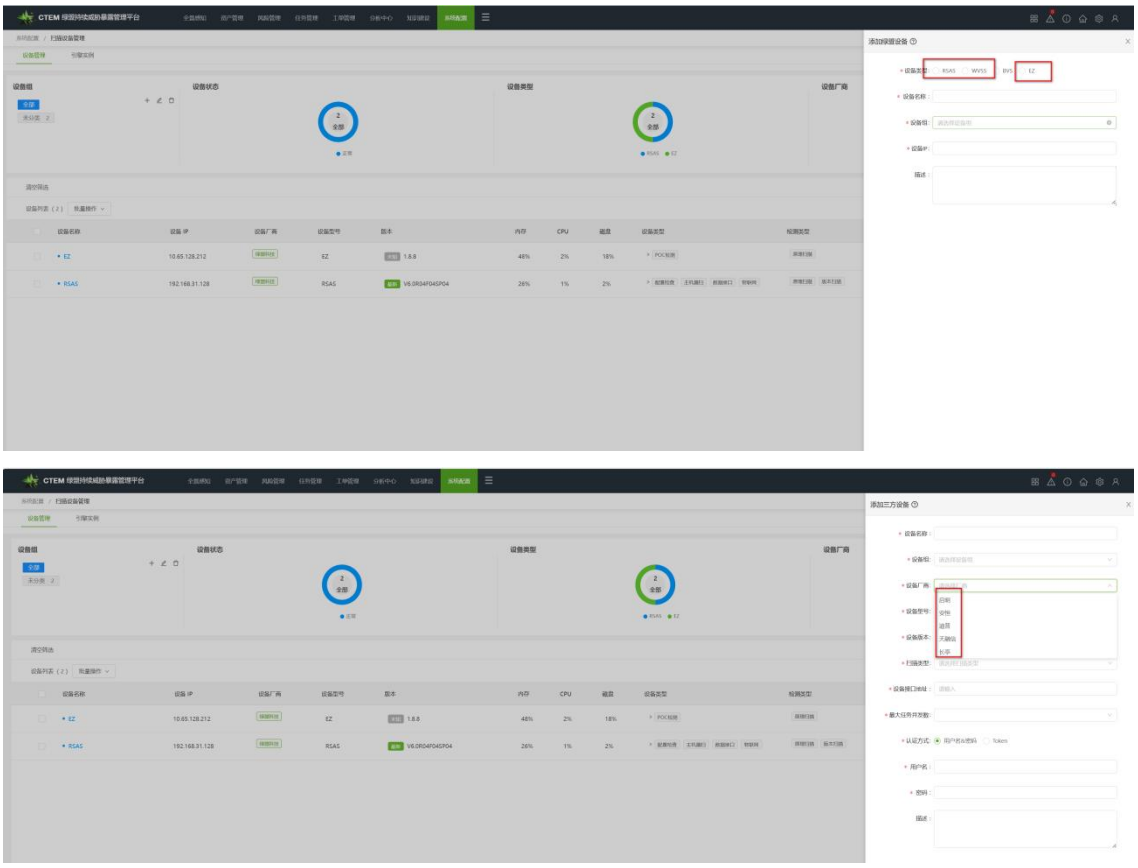
绿盟科技 CTEM 解决方案可以支持主动进行 Vite 相关资产和 CVE-2025-30208 漏洞风险的发现和排查：

用户使用外部攻击面发现功能将 CVE-2025-30208 漏洞线索同步至云端，通过资产测绘的方式获取目标单位的受影响资产。

通过指纹识别或 PoC 扫描进行测绘：




支持调用各类漏洞扫描设备：



# 五. 漏洞防护

## 5.1 官方升级

目前官方已发布新版本修复此漏洞，请受影响的用户尽快升级防护，下载链接：https://github.com/vitejs/vite/releases

## 5.2 产品防护

针对上述漏洞，绿盟科技 Web 应用防护系统（WAF）、网络入侵防护系统(IPS)与绿盟智能安全运营平台（ISOP）历史通用规则支持防护与研判，请相关用户升级规则包至最新版，以形成安全产品防护与监测能力。

产品规则升级的操作步骤详见如下链接：

WAF：https://mp.weixin.qq.com/s/7F8WCzWsuJ5T2E9e01wNog

IPS：https://mp.weixin.qq.com/s/DxQ3aaap8aujqZf-3VbNJg

## 5.3 临时防护措施

若相关用户暂时无法进行升级操作，可在不影响业务的前提下，通过对 Vite 开发服务器进行访问限制来临时缓解。

# 声明

本安全公告仅用来描述可能存在的安全问题，绿盟科技不为此安全公告提供任何保证或承诺。由于传播、利用此安全公告所提供的信息而造成的任何直接或者间接的后果及损失，均由使用者本人负责，绿盟科技以及安全公告作者不为此承担任何责任。

绿盟科技拥有对此安全公告的修改和解释权。如欲转载或传播此安全公告，必须保证此安全公告的完整性，包括版权声明等全部内容。未经绿盟科技允许，不得任意修改或者增减此安全公告内容，不得以任何方式将其用于商业目的。