ONEStor是否涉及 ChromeV8 越界写入和类型混淆漏洞（CVE-2024-4947）

存储配置 **刘路** 2024-06-30 发表

问题描述

ChromeV8(为谷歌开源的高性 能 Javascript 引擎，被广泛用于 Javascript 执行环境，如 浏览器等)存在越界写入漏洞(CVE-2024-4761)和类型混淆 漏洞(CVE-2024-4947)，可导致浏览器崩溃或执行任意代码， 危害等级均为高危

过程分析

Chrome V8 越界写入漏洞(CVE-2024-4761)。攻击 者可通过诱导用户打开恶意链接来利用该漏洞，成功利用后 可能造成内存破坏或者实现执行任意代码，进而导致浏览器 崩溃、获取主机权限等不安全行为。

Chrome V8 类型混淆漏洞(CVE-2024-4947)。攻击 者可通过诱导用户打开恶意链接来利用该漏洞，成功利用后 可能导致浏览器崩溃、信息泄露或在目标设备上执行任意代 码。

解决方法

当前ONEStor存储没有使用上述漏洞的相关组件，不涉及相关漏洞