关于 Google Chrome V8 存在类型混淆漏洞的安全公告

2025-07-16 16:42:49

安全公告编号:CNTA-2025-0010

2025 年 7 月 2 日，国家信息安全漏洞共享平台（CNVD）收录了 Google Chrome V8 类型混淆漏洞（CNVD-2025-14800，对应 CVE-2025-6554）。攻击者利用该漏洞，可通过诱骗用户访问恶意页面，实现远程代码执行攻击。目前，谷歌公司表示该漏洞已发现在野利用，并发布 Chrome 新版本。CNVD 建议受影响的单位和用户立即升级至最新版本。

一、漏洞情况分析

Google Chrome 是一款由谷歌公司开发的网页浏览器，该浏览器基于 WebKit、Mozilla 等开源软件开发，具有较好的性能、出色的兼容性和丰富的扩展程序，得到了广泛使用。

2025 年 7 月 2 日，国家信息安全漏洞共享平台（CNVD）收录了 Google Chrome V8 类型混淆漏洞。由于 Chrome 浏览器 V8 JavaScript（JS）引擎在处理 JS 代码时，对某些数据类型的边界检查和类型转换处理不当，导致浏览器无法正确区分不同类型的内存数据。攻击者通过精心构造包含特定 JS 表达式的恶意 Html 页面，并诱骗用户点击访问来触发此漏洞。未经授权的攻击者利用该漏洞，可远程对目标主机执行任意读写操作，并进一步实现远程代码执行攻击。

CNVD 对该漏洞的综合评级为“高危”。

二、漏洞影响范围

漏洞影响的产品和版本包括：

Google Chrome < 138.0.7204.96

基于 Chromium 内核开发的浏览器

三、漏洞处置建议

谷歌公司已紧急发布新版本修复该漏洞，各平台 Chrome 的修复版本情况如下：

1）Windows 版：Chrome v138.0.7204.96/.97

2）Linux 版：Chrome v138.0.7204.96

3）Mac 版：Chrome v138.0.7204.92/.93

Microsoft Edge、Brave、Opera 和 Vivaldi 等基于 Chromium 内核开发浏览器的安全更新仍在开发中。

CNVD 建议受影响的单位和用户立即将 Chrome 升级至最新版本，同时在使用 Chrome 时做好安全防范措施，谨慎访问来源不明的网页链接或文件。

参考链接：

https://chromereleases.googleblog.com/2025/06/stable-channel-update-for-desktop_30.html

https://issues.chromium.org/issues/427663123