关于 Google Chrome 存在沙箱逃逸漏洞的安全公告

2025-03-31 09:39:04

安全公告编号:CNTA-2025-0005

2025 年 3 月 28 日，国家信息安全漏洞共享平台（CNVD）收录了 Google Chrome 沙箱逃逸漏洞（CNVD-2025-06046，对应 CVE-2025-2783）。攻击者利用该漏洞可远程绕过 Chrome 的沙箱保护机制，造成信息泄露、代码执行等危害。目前，漏洞细节尚未公开，谷歌公司已发布新版本修复该漏洞。CNVD 建议受影响的用户尽快升级至最新版本。

一、漏洞情况分析

Chrome 是一款由谷歌公司开发的网页浏览器，具有较好的性能、出色的兼容性和丰富的扩展程序。Chrome 支持多标签页浏览，每个标签页都在独立的沙箱（SandBox）内运行，沙箱是 Chrome 的安全边界，用来隔离恶意代码对浏览器其他页面或用户系统的破坏，各标签页间的独立性提升了 Chrome 整体的稳定性和安全性。

2025 年 3 月 28 日，国家信息安全漏洞共享平台收录了 Google Chrome 沙箱逃逸漏洞。由于 Chrome 沙箱机制与 Windows 操作系统内核交互时存在逻辑错误缺陷，未经授权的攻击者可在远程条件下，利用该漏洞绕过 Chrome 的沙箱保护机制，造成信息泄露、代码执行等危害。攻击者综合利用该漏洞，可实现对目标主机的管理权限控制。

CNVD 对上述漏洞的综合评级为“高危”。

二、漏洞影响范围

漏洞影响的产品版本包括：

Google Chrome（Windows）< 134.0.6998.177

三、漏洞处置建议

目前，谷歌公司已发布新版本修复该漏洞，CNVD 建议受影响的用户尽快通过官方链接下载并更新至最新版本：

https://www.google.cn/chrome/

同时，CNVD 建议用户不要随意点击访问通过电子邮件、即时通讯软件等途径传播的不明网站链接或文件。

附参考链接：

https://www.kaspersky.com/about/press-releases/kaspersky-discovers-sophisticated-chrome-zero-day-exploit-used-in-active-attacks

https://chromereleases.googleblog.com/2025/03/stable-channel-update-for-desktop_25.html