Pagina 5 - New Chrome Zero-Day Actively Exploited; Google Issues Emergency Out-of-Band Patch

Classificações de Malware:

- exploit (Exploit)
- cve (Exploit)
- virus (Virus)
- infected (Virus)
- trojan (Trojan)
- adware (Adware)
- ads (Adware)
- backdoor (Backdoor)
- rat (Backdoor)
- ransomware (Ransomware)
- crypto (Ransomware)
- trojanized (Trojan)
- infection (Virus)

Google on Monday released out-of-band fixes to address three security issues in its Chrome browser, including
one that it said has come under active exploitation in the wild.The high-severity flaw is being tracked asCVE-
2025-5419(CVSS score: 8.8), and has been flagged as an out-of-bounds read and write vulnerability in the V8 Ja
vaScript and WebAssembly engine."Out-of-bounds read and write in V8 in Google Chrome prior to 137.0.7151.68 al
lowed a remote attacker to potentially exploit heap corruption via a crafted HTML page," reads thedescriptiono
f the bug on the NIST's National Vulnerability Database (NVD).Google credited Clement Lecigne and Benoit Seven
s of Google Threat Analysis Group (TAG) with discovering and reporting the flaw on May 27, 2025. It also noted
that the issue was addressed the next day by pushing out a configuration change to the Stable version of the
browser across all platforms.As is customary, the advisory is light on details regarding the nature of the att
acks leveraging the vulnerability or the identity of the threat actors perpetrating them. This is done so to e

nsure that a majority of users are updated with a fix and to prevent other bad actors from joining the exploit
ation bandwagon."Google is aware that an exploit for CVE-2025-5419 exists in the wild," the tech giantacknowle
dged.CVE-2025-5419 is the second actively exploited zero-day to be patched by Google this year afterCVE-2025-2
783(CVSS score: 8.3), which was identified by Kaspersky as being weaponized in attacks targeting organizations
in Russia.Users are recommended to upgrade to Chrome version 137.0.7151.68/.69 for Windows and macOS, and ver
sion 137.0.7151.68 for Linux to safeguard against potential threats. Users of Chromium-based browsers such as
Microsoft Edge, Brave, Opera, and Vivaldi are also advised to apply the fixes as and when they become availabl
e.Discover real-time defense tactics to detect and block deepfakes, fake domains, and multi-channel scams befo
re they cause damage.We'll unpack how leading teams are using AI, privacy-first design, and seamless logins to
earn user trust and stay ahead in 2025.Get the latest news, expert insights, exclusive resources, and strateg
ies from industry leaders all for free.

Link: https://thehackernews.com/2025/02/5-active-malware-campaigns-in-q1-2025.html