Google Chrome Hit by Second Zero-Day Attack

Severity: High **Date: 20 April 2023**

Description:

Google rolled out emergency fixes to address another actively exploited high-severity zero-day flaw in its Chrome web browser.

Impact:

The flaw, tracked as CVE-2023-2136, is described as a case of integer overflow in Skia, an open source 2D graphics library. Clément Lecigne of Google's Threat Analysis Group (TAG) has been credited with discovering and reporting the flaw on April 12, 2023.

"Integer overflow in Skia in Google Chrome prior to 112.0.5615.137 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page," according to the NIST's National Vulnerability Database (NVD).

Fix:

Recommended to upgrade to latest version 112.0.5615.137/138 for Windows, 112.0.5615.137 for macOS, and 112.0.5615.165 for Linux to mitigate 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 available.

Reference Links:

- https://thehackernews.com/2023/04/google-chrome-hit-by-second-zero-day.html
- https://www.timesnownews.com/technology-science/google-scrambles-to-fix-chromes-second-zero-day-exploit-in-just-days-update-now-article-99634624