CVE Report

ID: CVE-2024-4671
Summary: Use after free in Visuals in Google Chrome prior to 124.0.6367.201 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)
Created At: 2024-05-14T15:44:15Z
Updated At: 2024-07-03T02:07:53Z
CVSS v3: 9.6
Base Score: 9.6
Base Severity: CRITICAL
Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H
References:
https://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_9.html
https://issues.chromium.org/issues/339266700
https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/6G7EYH2JAK5OJPVNC6AXYQ5K7YGYNCDN/
https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/BWFSZNNWSQYDRYKNLBDGEXXKMBXDYQ3F/
https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/FAWEKDQTHPN7NFEMLIWP7YMIZ2DHF36N/
https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/NTSN22LNYXMWHVTYNOYQVOY7VDZFHENQ/
https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/WSUWM73ZCXTN62AT2REYQDD5ZKPFMDZD/
Descriptions:
en: Use after free in Visuals in Google Chrome prior to 124.0.6367.201 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)
es: Use after free en Visuals en Google Chrome anterior a 124.0.6367.201 permitió a un atacante remoto que había comprometido el proceso de renderizado realizar potencialmente un escape de la zona de pruebas a través de una página HTML manipulada. (Severidad de seguridad de Chrome: alta)