National Cyber Security Centre

2409020129-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical Google Chromium V8 Type Confusion Vulnerability (CVE-2024-7971, CVSSv3: 8.8)

Monday 2nd September, 2024

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.*
For more information on the Traffic Light Protocol, see https://www.first.org/tlp/.
Please treat this document in accordance with the TLP assigned.

Description

Published: 2024-08-21T21:15:00
Vendor: Google
Product: Chrome
CVE ID: CVE-2024-7971
CVSS3.x Score[1]**:** 8.8
EPSS[2]**:** 0.530430000
(For up to date EPSS score, click here: https://api.first.org/data/v1/epss?cve=CVE-2024-7971)

Summary: Type confusion in the V8 JavaScript and WebAssembly engine, impacting versions of Google Chromium prior to 128.0.6613.84, which allows a remote attacker to exploit heap corruption via a crafted HTML page (Chromium security severity: High). It has been observed **under active exploitation in the wild**.

Products Affected

- Google Chrome prior to 128.0.6613.84

Impact

Common Weakness Enumeration (CWE)[3]**:** Type confusion
Present in CISA Known Exploited Vulnerability(KEV)[4] **catalog:** YES
Used by Ransomware Operators: Known

Recommendations

The NCSC strongly advises affected organisations to review the latest release notes and install the relevant updates from Google.

Additional recommendations and mitigation's for CVE-2024-7971 can be found in the respective links below:

- https://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html
- https://issues.chromium.org/issues/360700873

[1] https://www.first.org/cvss/v3.0/specification-document
[2] https://www.first.org/epss/articles/prob_percentile_bins
[3] https://cwe.mitre.org/
[4] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
Tom Johnson House,
Beggars Bush,
Dublin, D04 K7X4,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre