



# CVE-2022-3652

Published on: Not Yet Published

Last Modified on: 12/09/2022 03:45:00 PM UTC

## CVE-2022-3652

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Chrome](#) from [Google](#) contain the following vulnerability:

Type confusion in V8 in Google Chrome prior to 107.0.5304.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)

CVE-2022-3652 has been assigned by [chrome-cve-admin@google.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Google](#) - **Chrome** version < 107.0.5304.62

CVSS3 Score: **8.8 - HIGH**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>REQUIRED</b>     |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

## CVE References

| Description                                                                          | Tags                                                                       | Link                                                                                                           |
|--------------------------------------------------------------------------------------|----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| Chrome Releases: Stable Channel Update for Desktop                                   | <a href="#">chromereleases.googleblog.com</a><br><a href="#">text/html</a> | <b>MISC</b><br><a href="#">chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_25.html</a> |
| 1369871 - chromium - An open-source project to help move the web forward. - Monorail | <a href="#">crbug.com</a><br><a href="#">text/html</a>                     | <b>MISC</b> <a href="#">crbug.com/1369871</a>                                                                  |

By selecting these links, you may be leaving CVEreport workspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](#).

## Related QID Numbers

[181168](#) Debian Security Update for chromium (DSA 5261-1)

[183055](#) Debian Security Update for chromium (CVE-2022-3652)

[377698](#) Google Chrome Prior to 107.0.5304.62 Multiple Vulnerabilities

[377720](#) Microsoft Edge Based on Chromium Prior to 107.0.1418.24 Multiple Vulnerabilities

[690969](#) Free Berkeley Software Distribution (FreeBSD) Security Update for chromium (b4ef02f4-549f-11ed-8ad9-3065ec8fd3ec)

## Known Affected Configurations (CPE V2.3)

| Type                            | Vendor                 | Product                | Version | Update | Edition | Language |
|---------------------------------|------------------------|------------------------|---------|--------|---------|----------|
| Application                     | <a href="#">Google</a> | <a href="#">Chrome</a> | All     | All    | All     | All      |
| cpe:2.3:a:google:chrome:*****:* |                        |                        |         |        |         |          |

No vendor comments have been submitted for this CVE

## Social Mentions

| Source                                                                                                                 | Title                                                                                                                                                    | Posted (UTC)           |
|------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
|  <a href="#">/r/k12cybersecurity</a> | <a href="#">MS-ISAC CYBERSECURITY ADVISORY – Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution – PATCH: NOW</a>         | 2022-10-26<br>13:00:35 |
|  <a href="#">/r/k12cybersecurity</a> | <a href="#">UPDATED MS-ISAC CYBERSECURITY ADVISORY – Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution – PATCH: NOW</a> | 2022-10-31<br>21:27:22 |
|  <a href="#">/r/netcve</a>           | <a href="#">CVE-2022-3652</a>                                                                                                                            | 2022-11-02<br>00:38:42 |

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)