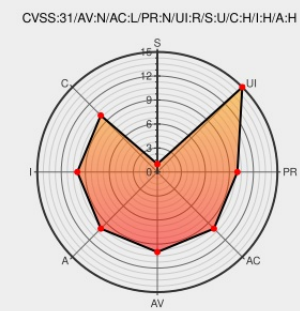
CVE-2022-3656

Published on: Not Yet Published

Last Modified on: 12/09/2022 03:07:00 PM UTC

CVE-2022-3656

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Chrome from Google contain the following vulnerability:

Insufficient data validation in File System in Google Chrome prior to 107.0.5304.62 allowed a remote attacker to bypass file system restrictions via a crafted HTML page. (Chromium security severity: Medium)

CVE-2022-3656 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
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
Chrome Releases: Stable Channel Update for Desktop	chromereleases.googleblog.com text/html	MISC chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_25.html
1345275 - chromium - An open-source project to help move the web forward. - Monorail	crbug.com text/html	MISC crbug.com/1345275

Related QID Numbers

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

183609 Debian Security Update for chromium (CVE-2022-3656)

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	Google	Chrome	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)
/r/k12cybersecurity	MS-ISAC CYBERSECURITY ADVISORY – Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution – PATCH: NOW	2022-10-26 13:00:35
/r/k12cybersecurity	UPDATED MS-ISAC CYBERSECURITY ADVISORY – Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution – PATCH: NOW	2022-10-31 21:27:22
/r/netcve	CVE-2022-3656	2022-11-02 00:38:45
/r/AICoinViews	The Imperva Red Team recently disclosed a vulnerability, dubbed CVE-2022-3656, affecting over 2.5 billion users of Google Chrome and Chromium-based browsers. This vulnerability allowed for the theft of sensitive files, such as crypto wallets and cloud provider credentials.	2023-01-13 06:10:15
/r/KibernetinisSaugumas	Dėl "SymStealer" pažeidžiamumo kyla pavojus kiekvienam "Google Chrome" naudotojui	2023-03-13 11:37:16

← Previous ID

Next ID→