



CVE-2015-1206

Published on: 10/06/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:09 PM UTC

CVE-2015-1206

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

Heap-based buffer overflow in Google Chrome before M40 allows remote attackers to cause a denial of service (unpaged memory write and process crash) via a crafted MP4 file.

CVE-2015-1206 has been assigned by security@google.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
bounties.csv · GitHub	Issue Tracking Third Party Advisory gist.github.com text/html	CONFIRM gist.github.com/bittorrent3389/8fee7cdaa73d1d351ee9

453979 - Security: UXSS in V8 - chromium - Monorail

Exploit

Issue Tracking

Patch

Vendor Advisory

bugs.chromium.org

text/html

CONFIRM

bugs.chromium.org/p/chromium/issues/detail?id=453979

444522 - Heap-buffer-overflow in ff_mov_read_stsd_entries - chromium - Monorail

Issue Tracking

Patch

Vendor Advisory

bugs.chromium.org

text/html

CONFIRM

bugs.chromium.org/p/chromium/issues/detail?id=444522

By selecting these links, you may be leaving CVEreport webspace. 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.

There are currently no QIDs associated with this CVE

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

← Previous ID

Next ID →