Copy Summary | View

Closed Bug 1450853 (CVE-2020-15666) Opened 5 years ago Closed 3 years ago

MediaError message property leaks cross-origin response status

Categories

Product: Core
Component: DOM: Security
Version: 58 Branch

Type: defect
Priority: P3 Severity: normal

Tracking

Status: RESOLVED FIXED
Milestone: mozilla80

Tracking Flags:	Tracking	Status
firefox-esr78	---	fixed
firefox80	---	fixed

People (Reporter: gunes.acar, Assigned: sstreich)

References

Details (Keywords: csectype-sop, parity-chrome, sec-low, Whiteboard: [domsecurity-backlog2][adv-main80+])

Attachments

error.png Details
5 years ago **roxleitan**
7.11 KB, image/png

Demo - Mediaerror message cross-origin response status leak Details
5 years ago **gunesacar**
77.31 KB, image/png

Demo source code - Mediaerror message cross-origin response status leak Details
5 years ago **gunesacar**
2.90 KB, text/html

Bug 1450853 - Use Generic Error for 3rdparty MediaElement r=ckerschb jcristau : **approval-mozilla-esr78+** Details | Review
3 years ago **Sebastian Streich [:sstreich]**
47 bytes, text/x-phabricator-request

advisory.txt Details
2 years ago **Tom Ritter [:tjr]**
448 bytes, text/plain

Bottom ↓ | Tags | Timeline

gunesacar Reporter
Description • 5 years ago

```
User Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:58.0) Gecko/20100101 Firefox/58.0
Build ID: 20180208173149

Steps to reproduce:

1- Visit: https://output.jsbin.com/nejatopusi
2- Enter a URL in the input box, click the "Test" button
The URL will be loaded as the `src` of an audio element.


Actual results:

The message property of the MediaError interface contains a different string for resources that loads
successfully. This allows an attacker to infer the response status for a cross-origin resource.



Expected results:

Cross-origin response status should not be detectable by scripts unless necessary CORS headers are sent by the
server.
```

gunesacar Reporter
Comment 1 • 5 years ago

```
Detecting cross-origin response status can be used in various attacks such as inferring login status to various
services, detecting servers on the LAN etc.

The following paper from 2015 gives an overview of attacks that are enabled by a similar AppCache-based
vulnerability: https://www.cc.gatech.edu/~slee3036/papers/lee:appcache.pdf
```

gunesacar Reporter
Comment 2 • 5 years ago

```
A clarification since this came up in the corresponding Chromium bug [1]: this attack works against any URL,
not only audio/video contents.

[1] https://crbug.com/828265 (restricted)
```

roxleitan
Comment 3 • 5 years ago

```
Hi gunesacar,

I cannot reproduce the issue using Firefox 58.0 (Build ID: 20180208173149) and the latest Nightly 61.0a1 on
Ubuntu 16.04 x64. (please see the attached screenshot)
```

Could you please retest the issue using the latest Firefox Release 59.0.2 and the latest Nightly 61.0a1 and report back the result? Consider using a new clean Firefox profile (https://goo.gl/AWo6h8) as well as safe mode (https://goo.gl/AR5o9d), to eliminate custom settings as a possible cause.

If the issue is reproducible on your end, would you please attach a screenshot of the error?

Thanks

Flags: needinfo?(gunes.acar)

roxleitan
Comment 4 • 5 years ago

*Attached image **error.png** — Details*

gunesacar Reporter
Comment 5 • 5 years ago

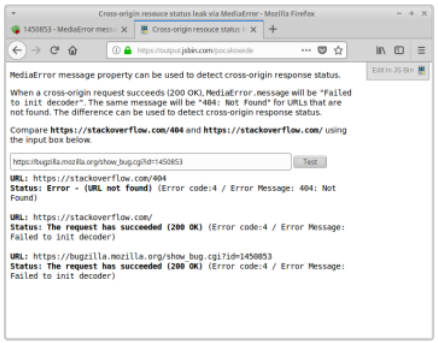
I think the message in the demo page wasn't very clear. The error message displayed in your screenshot ("Failed to init decoder") means the cross-origin response is succeeded (hence the `Status: Success`).

I updated the demo page to be more explicit. Will also attach a screenshot.
https://output.jsbin.com/pocakoxede

Flags: ~~needinfo?(gunes.acar)~~

gunesacar Reporter
Comment 6 • 5 years ago

*Attached image **Demo - Mediaerror message cross-origin response status leak** — Details*



gunesacar Reporter
Comment 7 • 5 years ago

*Attached file **Demo source code - Mediaerror message cross-origin response status leak** — Details*

Source code for the JSBin demo page at https://output.jsbin.com/pocakoxede

roxleitan
Updated • 5 years ago

Component: Untriaged → DOM: Security
Product: Firefox → Core

Daniel Veditz [:dveditz]
Updated • 5 years ago

Status: UNCONFIRMED → NEW
Ever confirmed: true
Keywords: csectype-sop, sec-low
Priority: -- → P3
See Also: → https://bugs.chromium.org/p/chromium/issues/detail?id=828265
Whiteboard: [domsecurity-backlog2]

gunesacar Reporter
Comment 8 • 5 years ago

Just FYI, this bug also allows an attacker to discover IoT or other devices on the local network by probing device-specific URLs (e.g. home automation API endpoints): https://freedom-to-tinker.com/2018/06/21/fast-web-based-attacks-to-discover-and-control-iot-devices/

This is similar to attacks that exploit side effects of <img> or similar passive elements', but can be used to detect web interfaces that do not contain images.

Discovered devices can then be attacked by DNS rebinding. All can be done in under ten seconds.

Tom Ritter [:tjr]
Updated • 3 years ago

Keywords: parity-chrome

Sebastian Streich [:sstreich] Assignee
Comment 9 • 3 years ago

*Attached file **Bug 1450853 - Use Generic Error for 3rdparty MediaElement r=ckerschb** — Details*

Phabricator Automation
Updated • 3 years ago

Assignee: nobody → sstreich
Status: NEW → ASSIGNED

Tom Ritter [:tjr]
Updated • 3 years ago

Flags: sec-bounty+

Pulsebot
Comment 11 • 3 years ago

Pushed by rmaries@mozilla.com:
https://hg.mozilla.org/integration/autoland/rev/6b518e88bdf9
Use Generic Error for 3rdparty MediaElement r=ckerschb,smaug

Razvan Maries
Comment 12 • 3 years ago • Edited

Backed out for perma failures.

Push with failure: https://treeherder.mozilla.org/#/jobs?repo=autoland&selectedTaskRun=dsGgzPx5TlutvoyheILWpA.0&resultStatus=pending%2Crunning%2Csuccess%2Ctestfailed%2Cbusted%2Cexception&searchStr=android%2C7.0%2Cx86-64%2Cwebrender%2Cdebug%2Creftests%2Ctest-android-em-7.0-x86_64-qr%2Fdebug-geckoview-crashtest-e10s%2Cc&revision=6b518e88bdf9f30c05c39694c134e16144293181

Logs:
https://treeherder.mozilla.org/logviewer.html#/jobs?job_id=309729753&repo=autoland&lineNumber=4285
https://treeherder.mozilla.org/logviewer.html#/jobs?job_id=309728609&repo=autoland&lineNumber=3752
https://treeherder.mozilla.org/logviewer.html#/jobs?job_id=309734962&repo=autoland&lineNumber=2289

Backout: https://hg.mozilla.org/integration/autoland/rev/df41fdf433a3624be684bd225eae90e3c452c509

Flags: needinfo?(sstreich)

Sebastian Streich [:sstreich] Assignee
Comment 13 • 3 years ago

Fixed the problem, reftest is now green :)

https://treeherder.mozilla.org/#/jobs?repo=try&revision=9ddfa699aae7de36ae3e5b71cf612837bb926388

Flags: ~~needinfo?(sstreich)~~

Pulsebot
Comment 14 • 3 years ago

Pushed by abutkovits@mozilla.com:
https://hg.mozilla.org/integration/autoland/rev/b8f37ab63181
Use Generic Error for 3rdparty MediaElement r=ckerschb,smaug

Andreea Pavel [:apavel]
Comment 15 • 3 years ago

bugherder

https://hg.mozilla.org/mozilla-central/rev/b8f37ab63181

Status: ASSIGNED → RESOLVED
Closed: 3 years ago
status-firefox80: --- → fixed
Resolution: --- → FIXED
Target Milestone: --- → mozilla80

Alex Catarineu (Tor Browser dev)
Comment 16 • 2 years ago

Comment on attachment 9157433 [details]
~~Bug 1450853~~ - Use Generic Error for 3rdparty MediaElement r=ckerschb

ESR Uplift Approval Request

- **If this is not a sec:{high,crit} bug, please state case for ESR consideration**: We would like to have this patch in the next Tor Browser 10 based on ESR78. Uplifting it would mean one less patch to backport for us.
- **User impact if declined**: Tor Browser devs will have to backport the patch on top of ESR78 branch.
- **Fix Landed on Version**: 80
- **Risk to taking this patch**: Low
- **Why is the change risky/not risky? (and alternatives if risky)**: The patch is minimal and only changes the error string for 3rd party loads.
- **String or UUID changes made by this patch**:

Attachment #9157433 - Flags: approval-mozilla-esr78?

Julien Cristau [:jcristau]
Comment 17 • 2 years ago

Comment on attachment 9157433 [details]
~~Bug 1450853~~ - Use Generic Error for 3rdparty MediaElement r=ckerschb

approved for 78.2esr

Attachment #9157433 - Flags: approval-mozilla-esr78? → approval-mozilla-esr78+

Julien Cristau [:jcristau]
Comment 18 • 2 years ago

bugherder uplift

https://hg.mozilla.org/releases/mozilla-esr78/rev/f46af8bc88a4

status-firefox-esr78: --- → fixed

Tom Ritter [:tjr]
Updated • 2 years ago

Whiteboard: [domsecurity-backlog2] → [domsecurity-backlog2][adv-main80+]

Tom Ritter [:tjr]
Comment 20 • 2 years ago

*Attached file **advisory.txt** — Details*

Tom Ritter [:tjr]
Updated • 2 years ago

Alias: CVE-2020-15666

Andreas Pehrson [:pehrsons]
Updated • 2 years ago

Blocks: ~~CVE-2021-23973~~