

Copy SummaryView

ClosedBug 1675905 (CVE-2020-26950)Opened 2 years agoClosed 2 years ago

Write side effects in MCallGetProperty opcode not accounted for

Categories

Product: CoreType: defectComponent: JavaScript Engine: JITPriority: Not setSeverity: --

Tracking

Status: VERIFIED FIXEDMilestone: 84 BranchTracking Flags: firefox-esr78firefox82firefox83firefox84Tracking: 82+verified+verified+verifiedStatus: verifiedverifiedverified

People (Reporter: tjr, Assigned: tcampbell)

Details (Keywords: csetype-jit, sec-critical, Whiteboard: [tfc-2020][sec-survey])

Attachments

exploit-details.zip2 years agoTom Ritter [tjr]1.81 KB, application/zipDetails

poc.html2 years agoFrederik Braun [freddy]1.04 KB, text/htmlDetails

Bug 1675905 - Simplify IonBuilder::createThisScripted. r?jandem,iain!2 years agoTed Campbell [tcampbell]47 bytes, text/x-phabricator-requestRyanVM : approval-mozilla-beta+RyanVM : approval-mozilla-release+RyanVM : approval-mozilla-esr78+tjr : sec-approval+Details | Review

JS shell test v22 years agoJan de Mooij [jandem]662 bytes, application/x-javascriptDetails

Crashtest for QA (FF78-84)2 years agoTed Campbell [tcampbell]1.01 KB, text/htmlDetails

advisory.txt2 years agoTom Ritter [tjr]281 bytes, text/plainDetails

Show Obsolete

BottomTagsTimeline

Multiple AuthorsDescription • 2 years ago • Edited

The root cause is in the |MIR.h| file and the opcode |MCallGetProperty|:

AliasSet getAliasSet() const override {if (!idempotent_) {return AliasSet::Store(AliasSet::Any);}return AliasSet::Load(AliasSet::ObjectFields | AliasSet::FixedSlot | AliasSet::DynamicSlot);}

if |idempotent_| is true, compiler will think this opcode does NOT have write side effect. But this is wrong.

In the function |createThisScripted|, it will emit a |MCallGetProperty| which |idempotent_| is true:

else {MCallGetProperty* callGetProp =MCallGetProperty::New(alloc(), newTarget, names().prototype);callGetProp->setIdempotent();getProto = callGetProp;}

It use this opcode to get callee.prototype, and this operatioin may call function |func_reslove| and write the |prototype| to slots, so it may be grow the slots buffer and update callee's slots buffer address. This will lead to UaF problem in JIT code as JIT code may be use the old buffer address after the grow.

https://twitter.com/TianfuCup/status/1324900642393976832

Tom Ritter [tjr]ReporterUpdated • 2 years ago

Group: core-security





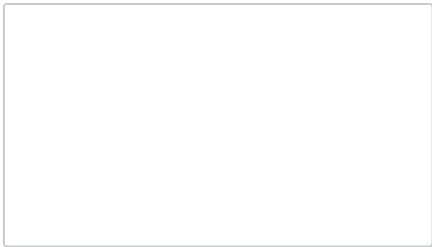



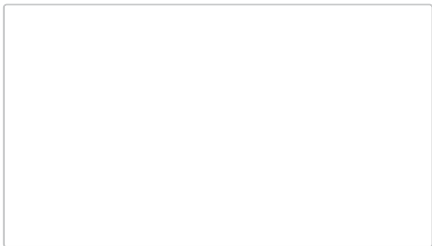



Tom Ritter [tjr]ReporterComment 1 • 2 years ago

Attached file exploit-details.zip — Details

Got this zip from them; awaiting the password.

Tom Ritter [tjr]ReporterComment 2 • 2 years ago

Password is tfc2020@cic@tfc2020

<div>  <div> Tom Ritter [tjr] Reporter </div> </div> <div>Updated • 2 years ago</div>	
<div>Component: Security → JavaScript Engine: JIT</div> <div>Summary: Tianfu Cup 2020 Exploit → Write side effects in MCallGetProperty opcode not accounted for</div>	
<div>  <div> Andrew McCreight [:mccr8] </div> </div> <div>Updated • 2 years ago</div>	
Group: core-security → javascript-core-security	
<div>  <div> Andrew McCreight [:mccr8] </div> </div> <div>Updated • 2 years ago</div>	
Keywords: csectype-jit	
<div>  <div> Frederik Braun [:freddy] </div> </div> <div>Comment 4 • 2 years ago</div>	
<div>Attached file poc.html — Details</div> <div>  </div>	
The zip file doesn't work trivially with all typical unzipers. Attaching PoC directly.	
<div>  <div> Ted Campbell [:tcampbell] Assignee </div> </div> <div>Comment 5 • 2 years ago</div>	
Attached file Bug 1675905 - Simplify IonBuilder::createThisScripted. r?jandem,iain! — Details	
<div>  <div> Jan de Mooij [jandem] </div> </div> <div>Comment 6 • 2 years ago</div>	
<div>Attached file JS-shell-testcase (obsolete) — Details</div> <div>I wrote a PoC based on theirs. Repros on m-c tip, debug build:</div> <div> <pre>\$ obj-shell-dbg/dist/bin/js --no-warp --no-threads poc.js poc.js:23:17 Error: Assertion failed: got -437918235, expected 2</pre> </div> <div>That's a poison value.</div>	
<div>  <div> Jan de Mooij [jandem] </div> </div> <div>Comment 7 • 2 years ago</div>	
<div>Attached file JS shell test v2 — Details</div> <div>  </div>	
This one triggers a crash in debug and opt builds.	
Attachment #9186451 - Attachment is obsolete: true	
<div>  <div> Jan de Mooij [jandem] </div> </div> <div>Comment 8 • 2 years ago</div>	
<div>Attached file Browser-test (obsolete) — Details</div> <div>Crashes content process in 82.0.2 on Mac.</div>	
<div>  <div> Ryan VanderMeulen [:RyanVM] </div> </div> <div>Comment 9 • 2 years ago</div>	
IIUC, this might not affect 83+ due to Warp being enabled, but I'll leave that for someone on the JS team to confirm and set.	
<div> status-firefox82: --- → affected status-firefox83: --- → ? status-firefox84: --- → ? status-firefox-esr78: --- → affected tracking-firefox82: --- → + tracking-firefox-esr78: --- → 82+ </div>	
<div>  <div> Ted Campbell [:tcampbell] Assignee </div> </div> <div>Comment 10 • 2 years ago</div>	

We should fix 83, because a warp/ion experiment is supposed to happen when release 83 ships.



Ryan VanderMeulen [RyanVM]
Comment 11 • 2 years ago



(In reply to Ted Campbell [tcampbell] from [comment #16](#))

We should fix 83, because a warp/ion experiment is supposed to happen when release 83 ships.

Thanks for confirming. Setting flags accordingly.

[status-firefox83](#): ? → [affected](#)
[status-firefox84](#): ? → [affected](#)
[tracking-firefox83](#): --- → +
[tracking-firefox84](#): --- → +



Phabricator Automation
Updated • 2 years ago



Assignee: nobody → tcampbell

[Attachment #9186450](#) - Attachment description: Bug 1675905 - Simplify IonBuilder::createThisScripted → Bug 1675905 - Simplify IonBuilder::createThisScripted. r?jandem!,iain!

Status: NEW → ASSIGNED



Phabricator Automation
Updated • 2 years ago



[Attachment #9186450](#) - Attachment description: Bug 1675905 - Simplify IonBuilder::createThisScripted. r?jandem!,iain! → Bug 1675905 - Simplify IonBuilder::createThisScripted. r?jandem!



Phabricator Automation
Updated • 2 years ago



[Attachment #9186450](#) - Attachment description: Bug 1675905 - Simplify IonBuilder::createThisScripted. r?jandem!,iain! → Bug 1675905 - Simplify IonBuilder::createThisScripted. r?jandem!,iain!



Ted Campbell [tcampbell] Assignee
Comment 12 • 2 years ago



Comment on [attachment 9186450 \[details\]](#)

[Bug 1675905](#) - Simplify IonBuilder::createThisScripted. r?jandem!,iain!

Security Approval Request

- **How easily could an exploit be constructed based on the patch?:** The patch suggests that `MCallGetProperty` is bad in this context, but doesn't directly point out the `fun_resolve` reallocation that is also needed to exploit. This aspect was novel to us and deriving from patch would require experience with jit exploitation.
- **Do comments in the patch, the check-in comment, or tests included in the patch paint a bulls-eye on the security problem?:** Unknown
- **Which older supported branches are affected by this flaw?:** ALL
- **If not all supported branches, which bug introduced the flaw?:** None
- **Do you have backports for the affected branches?:** Yes
- **If not, how different, hard to create, and risky will they be?:** Patch applies onto FF78 through 84
- **How likely is this patch to cause regressions; how much testing does it need?:** We are removing a very rare case that existed solely as a perf trick. Correctness risk of this patch is low, and primary risk is a performance cliff in rare cases. We've added a perf mitigation in this patch that avoids Ion in rare cases and sticks with the more predictable BaselineJIT.

[Attachment #9186450](#) - Flags: sec-approval?



Ted Campbell [tcampbell] Assignee
Comment 13 • 2 years ago



Comment on [attachment 9186450 \[details\]](#)

[Bug 1675905](#) - Simplify IonBuilder::createThisScripted. r?jandem!,iain!

ESR Uplift Approval Request

- **If this is not a sec(high,crit) bug, please state case for ESR consideration:** External report of sec-crit. TianFu Cup 2020.
- **User impact if declined:** Remote-code-execution in Content process.
- **Fix Landed on Version:**
- **Risk to taking this patch:** Low
- **Why is the change risky/not risky? (and alternatives if risky):** Correctness risk is low since we are removing a rare edge case added as a hypothetical performance fix. Performance risk is mitigated by an addition in this patch to rely on BaselineJIT in the very rare case instead of IonMonkey doing unnecessary compiles. The only place I've run into this rare case is heavily obfuscated JavaScript that is not performance critical.
- **String or UUID changes made by this patch:** None

[Attachment #9186450](#) - Flags: approval-mozilla-esr78?



Ted Campbell [tcampbell] Assignee
Comment 14 • 2 years ago




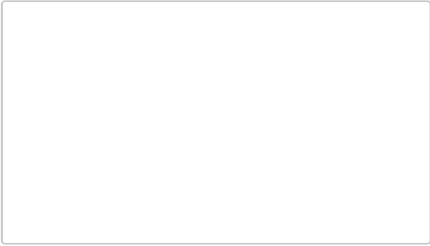














Comment on [attachment 9186450 \[details\]](#)

[Bug 1675905](#) - Simplify IonBuilder::createThisScripted. r?jandem!,iain!

Beta/Release Uplift Approval Request

- **User impact if declined:** External sec-crit. TianFu Cup 2020. Remote-code-execution in Content process.
- **Is this code covered by automated tests?:** Yes
- **Has the fix been verified in Nightly?:** No
- **Needs manual test from QE?:** Yes

<ul style="list-style-type: none">• If yes, steps to reproduce: See chemspill QA Plan. A crash-test HTML file is on bug. It may require 1-line tweaks for different versions.• List of other uplifts needed: None• Risk to taking this patch: Low• Why is the change risky/not risky? (and alternatives if risky): Correctness risk is low since we are removing a rare edge case added as a hypothetical performance fix. Performance risk is mitigated by an addition in this patch to rely on Baseline IT in the very rare case instead of IonMonkey doing unnecessary compiles. The only place I've run into this rare case is heavily obfuscated JavaScript that is not performance critical. Note: Affected code is off-by-default in 83+, so perf risk is very short lived.• String changes made/needed: None
<div>Attachment #9186450 - Flags: approval-mozilla-release?</div> <div>Attachment #9186450 - Flags: approval-mozilla-beta?</div>
<div><div><div><div><div></div><div>Ted Campbell [:tcampbell]</div></div><div>Assignee</div></div><div>Updated • 2 years ago</div></div><div>Flags: qe-verify+</div></div>
<div><div><div><div><div></div><div>Ted Campbell [:tcampbell]</div></div><div>Assignee</div></div><div>Comment 15 • 2 years ago</div></div><div><ul style="list-style-type: none">• ESR-78: Affected. Patch applies cleanly.• GeckoView-81: Affected. This previous version is still required for some mobile builds.• Release-82: Affected.• Beta-83: Disabled by default. A experiment is planned when this hits release that will re-enable Ion for a small population for limited time.• Nightly-84: Disabled by default.• Impacted code will be permanently removed from tree in Nightly-85.</div></div>
<div><div><div><div><div></div><div>Ted Campbell [:tcampbell]</div></div><div>Assignee</div></div><div>Comment 16 • 2 years ago</div></div><div><div>Attached file Crashtest for QA (FF78-84) — Details</div><div></div><div>Updated version of browser test with support for pre-82 and 82+ versions. On affected builds, this will crash tab. On fixed builds, this will render "Passed".</div></div></div>
<div>Attachment #9186453 - Attachment is obsolete: true</div>
<div><div><div><div><div></div><div>Ted Campbell [:tcampbell]</div></div><div>Assignee</div></div><div>Updated • 2 years ago</div></div><div>Attachment #9186486 - Attachment description: Crashtest for QA (FF72-84) → Crashtest for QA (FF78-84)</div></div>
<div><div><div><div><div></div><div>Tom Ritter [:tjr]</div></div><div>Reporter</div></div><div>Comment 17 • 2 years ago</div></div><div><div>Comment on attachment 9186450 [details]</div><div>Bug 1675905 - Simplify IonBuilder::createThisScripted. r?jandem!,iain!</div><div>sec-approved</div></div></div>
<div>Attachment #9186450 - Flags: sec-approval? → sec-approval+</div>
<div><div><div><div><div></div><div>Ryan VanderMeulen [:RyanVM]</div></div><div></div></div><div>Comment 18 • 2 years ago</div></div><div>https://hg.mozilla.org/mozilla-central/rev/8cdc2037b4b092157f1d04700bb09b00b19bbca6</div></div>
<div>Status: ASSIGNED → RESOLVED Closed: 2 years ago status-firefox84: affected → fixed Resolution: --- → FIXED Target Milestone: --- → 84 Branch</div>
<div><div><div><div><div></div><div>Ryan VanderMeulen [:RyanVM]</div></div><div></div></div><div>Comment 19 • 2 years ago</div></div><div><div>Comment on attachment 9186450 [details]</div><div>Bug 1675905 - Simplify IonBuilder::createThisScripted. r?jandem!,iain!</div><div>Approved for 83.0b10, 82.0.3, GV81, and 78.4.1esr.</div></div></div>
<div><div>Attachment #9186450 - Flags: approval-mozilla-release?</div><div>Attachment #9186450 - Flags: approval-mozilla-release+</div><div>Attachment #9186450 - Flags: approval-mozilla-esr78?</div><div>Attachment #9186450 - Flags: approval-mozilla-esr78+</div><div>Attachment #9186450 - Flags: approval-mozilla-beta?</div><div>Attachment #9186450 - Flags: approval-mozilla-beta+</div></div>

<div>  <div> Ryan VanderMeulen [:RyanVM] Comment 20 • 2 years ago </div> </div> <div>uplift</div>	<div>—</div>
https://hg.mozilla.org/releases/mozilla-beta/rev/f1da4198e696bbeb7c96e22ce1427655a173b243	
status-firefox83: affected → fixed	
<div>  <div> Ryan VanderMeulen [:RyanVM] Comment 21 • 2 years ago </div> </div> <div>uplift</div>	<div>—</div>
https://hg.mozilla.org/releases/mozilla-release/rev/861857e7c10478e180cc39a394377a3b1304954b (default) https://hg.mozilla.org/releases/mozilla-release/rev/6b20179fc7ae7932cd41cc522b01a9cdf5d6271a (GECKOVIEW_81_RELBRANCH)	
status-firefox82: affected → fixed	
<div>  <div> Ryan VanderMeulen [:RyanVM] Comment 22 • 2 years ago </div> </div> <div>uplift</div>	<div>—</div>
https://hg.mozilla.org/releases/mozilla-esr78/rev/f8c30263d78e8e1b20e5f59ef0cbfeabe17f6b6 (default) https://hg.mozilla.org/releases/mozilla-esr78/rev/22b8bef3c436a4d36b586804f342928e1ab11e51 (FIREFOX_ESR_78_4_X_RELBRANCH)	
status-firefox-esr78: affected → fixed	
<div>  <div> Tom Ritter [:tjr] Reporter Comment 23 • 2 years ago </div> </div>	<div>—</div>
Attached file advisory.txt (obsolete) — Details Attached is an advisory; if it can be improved please leave suggestions. Flags: needinfo?(jdemooij)	
<div>  <div> Tom Ritter [:tjr] Reporter Updated • 2 years ago </div> </div>	<div>—</div>
Alias: tfc-2020 → CVE-2020-26950 Whiteboard: [tfc-2020]	
<div>  <div> Tom Ritter [:tjr] Reporter Comment 24 • 2 years ago </div> </div>	<div>—</div>
Attached file advisory.txt — Details <div></div>	
Attachment #9186575 - Attachment is obsolete: true	
<div>  <div> Daniel Veditz [:dveditz] Comment 25 • 2 years ago </div> </div>	<div>—</div>
Some useful background from Ted in chat that I don't see here or in phabricator. Might be good history to preserve: <div> This issue is exactly the sort of problem that motivated the design of Warp. In two weeks, Warp will be shipped to release FF83 and we hopefully can put many of this family of security issues behind us. This issue has a lot in common with [the] 0-day at start of the Whistler 2019 and was the final straw that kicked off the Warp project. A huge congrats to @jandem and all the others for getting this designed, built, and shipped in less than a year. We've focused on the performance side mostly when discussing Warp, but improving security was one of the biggest motivations behind the scenes. </div>	
<div>  <div> Jan de Mooij [:jandem] Comment 26 • 2 years ago </div> </div>	<div>—</div>
(In reply to Tom Ritter [:tjr] (ni? for response to sec-[advisories/bounties/ratings/cves]) from comment #23) Attached is an advisory; if it can be improved please leave suggestions. Looks good to me, but the text is truncated at the end. Flags: needinfo?(jdemooij)	
<div>  <div> Daniel Cicas [:dcicas], Release QA Comment 27 • 2 years ago </div> </div>	<div>—</div>
Hello everybody! QA has managed to verify this issue on Win 10, Ubuntu 18 and mac OS (Cristi Fogel thank you!). We managed to verify this bug on Fx 83.0b10, Nightly 84.0a1 (BuildID:20201108093650), Fx 82.0.3, Fx DevEd 83.0b10 and Firefox esr treeherder build (https://treeherder.mozilla.org/jobs?repo=mozilla-esr78&revision=f8c30263d78e8e1b20e5f59ef0cbfeabe17f6b6). Once esr is officially built we can have a quick pass at it if you feel its necessary. Status: RESOLVED → VERIFIED	

[status-firefox82: fixed](#) → [verified](#)
[status-firefox83: fixed](#) → [verified](#)
[status-firefox84: fixed](#) → [verified](#)
[status-firefox-esr78: fixed](#) → [verified](#)
Flags: ~~ee-verify~~



Oana Horvath [:ohorvath]

Comment 28 • 2 years ago • [Edited](#)



The bug fix was also verified on mobile on the following builds and devices:

- versions: Nightly 84, Beta 83.0.0-beta.4 & RC 82.1.3, Focus Beta 8.8.4
- devices: Xiaomi Mi Pad 2 (Android 5.1, x86), OnePlus A3 (Android 6.0.1), Nexus 9 (Android 7.1.1), Motorola Moto G6 (Android 8), Google Pixel 3a (Android 11), Huawei Mate 20 Lite (Android 10).



Daniel Cicas [:dcicas], Release QA

Comment 29 • 2 years ago • [Edited](#)



Hello,

Verified the official esr 78.5.0 for good measure. No issues.



Release mgmt bot [:suhail / :marco / :calixte]

Comment 30 • 2 years ago



As part of a security bug pattern analysis, we are requesting your help with a high level analysis of this bug. It is our hope to develop static analysis (or potentially runtime/dynamic analysis) in the future to identify classes of bugs.

Please visit [this google form](#) to reply.

Flags: needinfo?(tcampbell)

Whiteboard: [tfc-2020] → [tfc-2020][sec-survey]



Ted Campbell [:tcampbell]

Updated • 2 years ago

[Assignee](#)



Flags: ~~needinfo?(tcampbell)~~



Daniel Veditz [:dveditz]

Updated • 2 years ago



Group: javascript-core-security → core-security-release



Daniel Veditz [:dveditz]

Updated • 2 years ago



Group: ~~core-security-release~~

You need to [log in](#) before you can comment on or make changes to this bug.

Top ↑