Closed Bug 1933023 (CVE-2025-0241) Opened 1 year ago Closed 1 year ago

Assertion failure: has<CharT>(), at js/src/builtin/intl/Segmenter.h:141

Categories

Product: Core
Component: JavaScript: Internationalization API
Type: defect
Priority: P2 Severity: S3

Tracking

Status: RESOLVED FIXED
Milestone: 135 Branch

Tracking Flags:

	Tracking	Status
firefox-esr115	---	unaffected
firefox-esr128	134+	fixed
firefox133	---	wontfix
firefox134	+	fixed
firefox135	+	fixed

People (Reporter: sm-bugs, Assigned: jandem)

References (Blocks 2 open bugs, Regression)

Details (Keywords: regression, reporter-external, sec-moderate, Whiteboard: [adv-main134+][adv-ESR128.6+])

Attachments

Bug 1933023 - Check whether the segment's chars are Latin1 instead of the JS string. r?anba! — pascalc : **approval-mozilla-beta+** — Details | Review
1 year ago **Jan de Mooij [:jandem]**
48 bytes, text/x-phabricator-request

Bug 1933023 - Add test. r?anba! — Details | Review
1 year ago **Jan de Mooij [:jandem]**
48 bytes, text/x-phabricator-request

Steps to reproduce:

Version: `ee42ec590725439d33792bc8657d60f080786b2e`
Args: `js --fuzzing-safe <test-case>`
Test case:

```
a = {
  "twoByte" : true}
b = newString("12345678901234567890", a)
c = Intl.Segmenter
d = new c
e = d.segment(b)
e.containing()
f = {}
Object.defineProperty(f, "12345678901234567890",
                      {value : e})[b].containing()
```

Actual results:

```
Assertion failure: has<CharT>(), at js/src/builtin/intl/Segmenter.h:141

#0 0x557462a3e128 in unsigned char* js::SegmentsStringChars::data<unsigned char>() c
#1 0x557462a3e128 in auto* CreateBreakIterator<GraphemeClusterSegmenterBreakIterator
#2 0x557462a3e128 in bool EnsureBreakIterator<js::SegmentsObject>(JSContext*, JS::Ha
#3 0x557462a3e128 in js::ArrayObject* FindSegmentBoundaries<js::SegmentsObject>(JSCo
#4 0x557462a3e128 in js::intl_FindSegmentBoundaries(JSContext*, unsigned int, JS::Va
#5 0x55746216521e in CallJSNative(JSContext*, bool (*)(JSContext*, unsigned int, JS:
#6 0x55746216447f in js::InternalCallOrConstruct(JSContext*, JS::CallArgs const&, js
#7 0x55746217ea1c in js::CallFromStack(JSContext*, JS::CallArgs const&, js::CallReas
#8 0x55746217ea1c in js::Interpret(JSContext*, js::RunState&) js/src/vm/Interpreter.
#9 0x5574621632b3 in js::RunScript(JSContext*, js::RunState&) js/src/vm/Interpreter.
```

Nils Bars Reporter
Updated • 1 year ago

Blocks: 1903968
Group: firefox-core-security → core-security
Component: Untriaged → JavaScript Engine
Product: Firefox → Core
Version: Firefox 132 → Trunk

Ryan VanderMeulen [:RyanVM]
Updated • 1 year ago

Group: core-security → javascript-core-security
Component: JavaScript Engine → JavaScript: Internationalization API

Daniel Veditz [:dveditz]
Updated • 1 year ago

Keywords: reporter-external

Jan de Mooij [:jandem] Assignee
Updated • 1 year ago

Flags: needinfo?(jdemooij)

Jan de Mooij [:jandem] Assignee
Comment 1 • 1 year ago • Edited

Reduced test below.

The segments object has the JS string and `SegmentsStringChars`. The JS string is initially a two-byte string but is later turned into a Latin1 atom-ref string. This confuses `EnsureBreakIterator`.

```
var str = "12345678901234567890";
var strTwoByte = newString(str, {twoByte: true});
```

Jan de Mooij [:jandem] Assignee
Comment 2 • 1 year ago

Attached file ***Bug 1933023 - Check whether the segment's chars are Latin1 instead of the JS string. r?anba!*** — *Details*

Ryan VanderMeulen [:RyanVM]
Updated • 1 year ago

status-firefox133: --- → wontfix
status-firefox134: --- → affected
status-firefox135: --- → affected
status-firefox-esr115: --- → unaffected
status-firefox-esr128: --- → affected
Keywords: regression
Regressed by: ~~1423593~~

André Bargull [:anba]
Comment 3 • 1 year ago

Regression from ~~bug 1881995~~.

Regressed by: ~~1881995~~
No longer regressed by: ~~1423593~~

Jan de Mooij [:jandem] Assignee
Comment 4 • 1 year ago

Yes this goes back to atom-refs (~~bug 1881995~~) but was uncovered by the patch for ~~bug 1928407~~ because it added this assertion.

I'm not sure what security rating to give this. We call into ICU4X with the wrong character type but I don't know if it's exploitable. Interpreting a `char16_t` buffer as an `unsigned char` buffer probably doesn't read out-of-bounds memory, but I don't know what else ICU4X is doing with the string chars.

We should probably uplift bug 1928407 and this patch to ESR 128.

Jan de Mooij [:jandem] Assignee
Comment 5 • 1 year ago

Attached file ***Bug 1933023 - Add test. r?anba!*** — *Details*

Bryan Thrall [:bthrall]
Updated • 1 year ago

Blocks: sm-security
Severity: -- → S3
Priority: -- → P2

Jan de Mooij [:jandem] Assignee
Comment 6 • 1 year ago

Attached file ***Bug 1933023 (patch for ESR128) - Check whether the segment's chars are Latin1 instead of the JS string. r?anba!*** — *Details*

This also has the patch for ~~bug 1928407~~ folded into it.

Phabricator Automation
Updated • 1 year ago

Attachment #9440175 - Flags: approval-mozilla-esr128?

Jan de Mooij [:jandem] Assignee
Comment 7 • 1 year ago

Comment on attachment 9439717 [details]
~~Bug 1933023~~ - Check whether the segment's chars are Latin1 instead of the JS string. r?anba!

Beta/Release Uplift Approval Request

- **User impact if declined/Reason for urgency**: Broken websites and maybe crashes or security issues.
- **Is this code covered by automated tests?**: 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 and pretty self-contained.
- **String changes made/needed:**
- **Is Android affected?**: Yes

Attachment #9439717 - Flags: approval-mozilla-beta?

Pulsebot
Comment 8 • 1 year ago

Pushed by jdemooij@mozilla.com:
https://hg.mozilla.org/integration/autoland/rev/ee678c4855f6
Check whether the segment's chars are Latin1 instead of the JS string. r=anba

Donal Meehan [:dmeehan]
Updated • 1 year ago

tracking-firefox134: --- → +
tracking-firefox135: --- → +
tracking-firefox-esr128: --- → 134+

Sebastian Hengst [:aryx] (needinfo me if it's about an intermittent or backout)
Comment 9 • 1 year ago

https://hg.mozilla.org/mozilla-central/rev/ee678c4855f6

Group: javascript-core-security → core-security-release
Status: ASSIGNED → RESOLVED
Closed: 1 year ago
status-firefox135: affected → fixed
Resolution: --- → FIXED
Target Milestone: --- → 135 Branch

Pulsebot
Comment 10 • 1 year ago

uplift

https://hg.mozilla.org/releases/mozilla-beta/rev/5d99b1e691ac

Pascal Chevrel:pascalc
Updated • 1 year ago

Jan de Mooij [:jandem] Assignee
Updated • 1 year ago

Flags: needinfo?(jdemooij)

Daniel Veditz [:dveditz]
Updated • 1 year ago

Flags: sec-bounty? → sec-bounty+

Ryan VanderMeulen [:RyanVM]
Comment 11 • 1 year ago

Comment on attachment 9440175 [details]
~~Bug 1933023~~ (patch for ESR128) - Check whether the segment's chars are Latin1 instead of the JS string. r? anba!

Approved for 128.6esr.

Attachment #9440175 - Flags: approval-mozilla-esr128? → approval-mozilla-esr128+

Ryan VanderMeulen [:RyanVM]
Updated • 1 year ago

status-firefox-esr128: affected → fixed

Pulsebot
Comment 12 • 1 year ago

uplift

https://hg.mozilla.org/releases/mozilla-esr128/rev/0a63d2eb669e

Frederik Braun [:freddy]
Updated • 1 year ago

```
Memory corruption when using JavaScript Text Segmentation
Nils Bars

When segmenting specially crafted text, segmentation would
```

Frederik Braun [:freddy]
Updated • 1 year ago

Alias: CVE-2025-0241

Pulsebot
Comment 14 • 1 year ago

Pushed by jdemooij@mozilla.com:
https://hg.mozilla.org/integration/autoland/rev/8d4783ce33d3
Add test. r=anba

Jan de Mooij [:jandem] Assignee
Updated • 1 year ago

Flags: ~~needinfo?(jdemooij)~~

Sebastian Hengst [:aryx] (needinfo me if it's about an intermittent or backout)
Comment 15 • 1 year ago

Top ↑