Closed Bug 1929156 (CVE-2025-0239) Opened 1 year ago Closed 1 year ago

Only the first Alt-Svc ALPN negotiation is verified

Categories

Product: Core
Component: Networking

Type: defect

Priority: P1 Severity: S2

Tracking

Status: VERIFIED FIXED

Milestone: 135 Branch

Tracking Flags:

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

People (Reporter: pspaul95+bugzilla, Assigned: valentin)

References

Details (Keywords: csectype-sop, reporter-external, sec-moderate, Whiteboard: [client-bounty-form][necko-triaged][necko-priority-queue][adv-main134+][adv-ESR128.6+])

Attachments

alt-svc-reproducer.zip Details
1 year ago **Frederik Braun [:freddy]**
7.78 KB, application/zip

Bug 1929156 - Check negotiated ALPN matches altSvc protocol r=#necko tjr : **sec-approval+** Details | Review
1 year ago **Valentin Gosu [:valentin]**
48 bytes, text/x-phabricator-request

Bug 1929156 - Test that ALPN token is checked r=#necko Details | Review
1 year ago **Valentin Gosu [:valentin]**
48 bytes, text/x-phabricator-request

Bug 1929156 - Check negotiated ALPN matches altSvc protocol r=#necko phab-bot : **approval-mozilla-beta+** Details | Review
1 year ago **Valentin Gosu [:valentin]**
48 bytes, text/x-phabricator-request

Terminal output Win11, macOS13, Ubuntu22.04.txt Details
1 year ago Bianca Hidecuti, Desktop Test Engineering [:bhidecuti]
1.86 KB, text/plain

Bug 1929156 - Check negotiated ALPN matches altSvc protocol r=#necko phab-bot : **approval-mozilla-esr128+** Details | Review
1 year ago **Valentin Gosu [:valentin]**
48 bytes, text/x-phabricator-request

advisory.txt Details
1 year ago **Frederik Braun [:freddy]**
187 bytes, text/plain

Bottom ↓ Tags ▾ Timeline ▾

pspaul Reporter
Description • 1 year ago

Version: Firefox 131.0.3 (64-bit)
OS: Manjaro Linux 24.1.1

How was this issue discovered?
Manual testing. I was researching cross-protocol attacks using the Alt-Svc header when I found this bypass.

General Description:

The Alt-Svc spec's section 2.4 (https://httpwg.org/specs/rfc7838.html#switching) mandates that the browser verifies that the alternative service negotiates the correct protocol, for example via ALPN:

> If the connection to the alternative service does not negotiate the expected protocol (for example, ALPN fails to negotiate h2, or an Upgrade request to h2c is not accepted), the connection to the alternative service MUST be considered to have failed.

Firefox only verifies this for the first connection but not for subsequent ones. Therefore, a Man-in-the-Middle attacker can bypass the ALPN check by forwarding the first connection to a valid server, closing the connection after some time, and forwarding all subsequent requests to a different server.

The PoC demonstrates this by running three TLS servers, all using the same certificate:

- HTTP/1.1 on port `:8443` (ALPN offers `http1.1`)
- HTTP/2 on port `:8444` (ALPN offers `h2`)
- Plain TLS on port `:8445` (ALPN list is empty)

Firefox should never use the alternative service `h2=":8445"` because ALPN will not negotiate `h2`. However, by forwarding the first request to `:8444`, which correctly negotiates `h2`, Firefox can be tricked into trusting all later connections.

Steps to reproduce:

1. Start the PoC: `node server.js`
2. Add `127.0.0.1 foo.example.com` to your `/etc/hosts` file
3. Visit `https://foo.example.com:8443/?alt-svc=:1337` in Firefox

4. Accept the self-signed certificate warning (or replace `privkey.pem` and `fullchain.pem` with valid certificates before step 1)
5. Now the following should happen:
   i. The page will first be served via HTTP/1.1 over TLS from `:8443`, delivering the `Alt-Svc: h2=":1337"` header
   ii. After 1 second, the page refreshes, causing the browser to make the first connection to the attacker's alternative service on `:1337`
   iii. The attacker forwards this first request to the legitimate HTTP/2 server on `:8444`
   iv. The new page loads, showing that it was loaded via HTTP/2
   v. The attacker now closes the forwarded connection between the browser and the HTTP/2 server
   vi. The page then refreshes again, causing the browser to open a new connection to the attacker on `:1337`
   vii. The attacker now forwards the request to the invalid TLS server at `:8445`
   viii. The page loads, showing that it was loaded from `:8445`, which shouldn't happen

The PoC script's output should demonstrate the same:

```
[h1] GET /?alt-svc=:1337
[attacker] Forwarding to h2 (:8444)
[h1] GET /favicon.ico
[h2] GET /?refresh
[attacker] Terminating first connection
[attacker] Forwarding to plain (:8445)
[plain] Got connection
[plain] Got data: GET / HTTP/1.1
[plain] Got data: Host: foo.example.com:8443
[plain] Got data: User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:131.0) Gecko/201001
...
```

I also recorded a demo of the PoC, I hope you enjoy it ;)

Root cause analysis:

I'm not very familiar with the Firefox code base, but it looks like `TRRServiceChannel::BeginConnect()` is consulting the Alt-Svc cache here: https://searchfox.org/mozilla-central/rev/387f3edbef37d31b2e91fb0812c74b54729e86ff/netwerk/protocol/http/TRRServiceChannel.cpp#405-407

If there's a matching entry, it means that the alternative service was previously validated, and Firefox connects to the `mConnectionInfo` from the cache entry instead of the original one.

I think the problem here is that the Alt-Svc cache holds the validation state. To me, the spec sounds like each new TLS connection needs to do the validation individually to prevent a Man-in-the-Middle attacker

from switching the destination server at some point.

Flags: sec-bounty?

Frederik Braun [:freddy]
Comment 1 • 1 year ago

*Attached file **alt-svc-reproducer.zip** — Details*

Looks like the attachment did not make it through yet. Submitting for pspaul.

Frederik Braun [:freddy]
Comment 2 • 1 year ago

Profile when running the test case

Andrew McCreight [:mccr8]
Updated • 1 year ago

Group: firefox-core-security → network-core-security
Component: Security → Networking
Product: Firefox → Core

Valentin Gosu [:valentin] Assignee
Comment 3 • 1 year ago

*Attached file **Bug 1929156 - Check negotiated ALPN matches altSvc protocol r=#necko** — Details*

Daniel Veditz [:dveditz]
Updated • 1 year ago

Status: UNCONFIRMED → NEW
Ever confirmed: true
Keywords: csectype-sop, sec-high

Valentin Gosu [:valentin] Assignee
Updated • 1 year ago

Severity: -- → S2
Priority: -- → P1
Whiteboard: [client-bounty-form] → [client-bounty-form][necko-triaged]

Valentin Gosu [:valentin] Assignee
Updated • 1 year ago

Assignee: nobody → valentin.gosu

Greg Hess

Updated • 1 year ago

Whiteboard: [client-bounty-form][necko-triaged] → [client-bounty-form][necko-triaged][necko-priority-queue]

Phabricator Automation
Updated • 1 year ago

Attachment #9435935 - Attachment description: WIP: Bug 1929156 - Check negotiated ALPN matches altSvc protocol r=#necko → Bug 1929156 - Check negotiated ALPN matches altSvc protocol r=#necko

Valentin Gosu [:valentin] Assignee
Comment 4 • 1 year ago

Attached file ***Bug 1929156 - Test that ALPN token is checked r=#necko*** *— Details*

Valentin Gosu [:valentin] Assignee
Comment 5 • 1 year ago

Comment on attachment 9435935 [details]
~~Bug 1929156~~ - Check negotiated ALPN matches altSvc protocol r=#necko

Security Approval Request

- **How easily could an exploit be constructed based on the patch?**: Relatively easily.
- **Do comments in the patch, the check-in comment, or tests included in the patch paint a bulls-eye on the security problem?**: Yes
- **Which branches (beta, release, and/or ESR) are affected by this flaw, and do the release status flags reflect this affected/unaffected state correctly?**: 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?**: Applies cleanly to all branches
- **How likely is this patch to cause regressions; how much testing does it need?**: Unlikely to cause regressions.
- **Is the patch ready to land after security approval is given?**: Yes
- **Is Android affected?**: Yes

Attachment #9435935 - Flags: sec-approval?

Tom Ritter [:tjr]
Comment 6 • 1 year ago

Do I understand correctly that exploiting this would require an unusual server configuration that is likely extremely uncommon?

Flags: needinfo?(valentin.gosu)

Valentin Gosu [:valentin] Assignee
Comment 7 • 1 year ago

(In reply to Tom Ritter [:tjr] from ~~comment #6~~)

> Do I understand correctly that exploiting this would require an unusual server configuration that is likely extremely uncommon?

Yes, the original server needs to provide an alt-svc directing the browser to a port it doesn't control. And even so, TLS is still required, so I'm not sure how much damage the attacker could do.

Flags: ~~needinfo?(valentin.gosu)~~

Tom Ritter [:tjr]
Comment 8 • 1 year ago

Comment on attachment 9435935 [details]
~~Bug 1929156~~ - Check negotiated ALPN matches altSvc protocol r=#necko

Approved to land and uplift

Attachment #9435935 - Flags: sec-approval? → sec-approval+

Ryan VanderMeulen [:RyanVM]
Updated • 1 year ago

status-firefox133: --- → wontfix
status-firefox134: --- → affected
status-firefox135: --- → affected
status-firefox-esr115: --- → affected
status-firefox-esr128: --- → affected
tracking-firefox134: --- → +
tracking-firefox135: --- → +
tracking-firefox-esr115: --- → 134+
tracking-firefox-esr128: --- → 134+

Pulsebot
Comment 9 • 1 year ago

Pushed by valentin.gosu@gmail.com:
https://hg.mozilla.org/integration/autoland/rev/db100843b0f0
Check negotiated ALPN matches altSvc protocol r=necko-reviewers,kershaw

Sebastian Hengst [:aryx] (needinfo me if it's about an intermittent or backout)
Comment 10 • 1 year ago

https://hg.mozilla.org/mozilla-central/rev/db100843b0f0

Status: NEW → RESOLVED
Closed: 1 year ago
status-firefox135: affected → fixed
Resolution: --- → FIXED
Target Milestone: --- → 135 Branch

Valentin Gosu [:valentin] Assignee
Comment 11 • 1 year ago

Attached file ***Bug 1929156 - Check negotiated ALPN matches altSvc protocol r=#necko*** *— Details*

Original Revision: https://phabricator.services.mozilla.com/D228217

Phabricator Automation
Updated • 1 year ago

Attachment #9441550 - Flags: approval-mozilla-beta?

Ryan VanderMeulen [:RyanVM]
Updated • 1 year ago

Group: network-core-security → core-security-release

Phabricator Automation
Comment 12 • 1 year ago

beta Uplift Approval Request

- **User impact if declined**: An attacker could make Firefox use a different protocol than the one specified in the ALPN header.
- **Code covered by automated testing**: yes
- **Fix verified in Nightly**: yes
- **Needs manual QE test**: yes
- **Steps to reproduce for manual QE testing**: see ~~comment 0~~
- **Risk associated with taking this patch**: medium
- **Explanation of risk level**: Our code coverage for this isn't great. I'm not 100% sure our ALPN negotiation doesn't have any bugs that would cause us to fail loading websites in specific circumstances.
- **String changes made/needed**: none
- **Is Android affected?**: yes

Flags: qe-verify+

Daniel Veditz [:dveditz]
Comment 13 • 1 year ago

I misunderstood this as a certificate check bypass. Lowering to sec-moderate

Keywords: sec-high → sec-moderate

Daniel Veditz [:dveditz]
Updated • 1 year ago

Flags: sec-bounty? → sec-bounty+

Mihai Boldan, Desktop QA [:mboldan]
Updated • 1 year ago

QA Whiteboard: [qa-triaged]

Phabricator Automation
Updated • 1 year ago

Attachment #9441550 - Flags: approval-mozilla-beta? → approval-mozilla-beta+

Pulsebot
Comment 14 • 1 year ago

uplift

`https://hg.mozilla.org/releases/mozilla-beta/rev/34b0d8d04644`

Lando Automation
Updated • 1 year ago

status-firefox134: affected → fixed

Bianca Hidecuti, Desktop Test Engineering [:bhidecuti]
Comment 15 • 1 year ago

Attached file ***Terminal output Win11, macOS13, Ubuntu22.04.txt*** *— Details*

I was able to reproduce the issue on Firefox 131.0.3 using Windows 11, macOS 13.6 and Ubuntu 22.04, as described in ~~Comment 0~~.
Verified this with Firefox Nightly 135.0a1 (2024-12-05) and with Firefox 134.0b7 (treeherder build from ~~Comment 14~~) on the previously mentioned OSes and after accessing https://foo.example.com:8443/?alt-svc=:1337, the browser traffic is redirected as follows:

- from ALPN=http/1.1 (:8443) to ALPN=h2 (:8444) and then back to ALPN=http/1.1 (:8443).

Regarding the terminal/cmd output, we noticed that when the attacker executes "[attacker] Forwarding to plain (:8445)", the process is automatically interrupted on the fixed builds:

- either the server shuts down (on macOS/Windows)
- or logs stop appearing (on Ubuntu).

I will attach a file with the script output. @valentin, could you please take a look at the output and let us know if the results are as expected? Thank you in advance!

Flags: needinfo?(valentin.gosu)

Valentin Gosu [:valentin] Assignee
Comment 16 • 1 year ago

Thank you, Bianca. That is the expected behaviour.

Flags: ~~needinfo?(valentin.gosu)~~

Bianca Hidecuti, Desktop Test Engineering [:bhidecuti]
Comment 17 • 1 year ago

Thank you for the confirmation!
Based on ~~Comment 15~~ and 16 I am marking this verified as fixed on the previously mentioned versions.

status-firefox134: fixed → verified
status-firefox135: fixed → verified
Flags: ~~qe-verify+~~

Ryan VanderMeulen [:RyanVM]
Comment 18 • 1 year ago

Please nominate this for ESR128 approval also.

status-firefox-esr115: affected → wontfix
tracking-firefox-esr115: 134+ → -
Flags: needinfo?(valentin.gosu)

Valentin Gosu [:valentin] Assignee
Comment 19 • 1 year ago

Attached file ***Bug 1929156 - Check negotiated ALPN matches altSvc protocol r=#necko*** — *Details*

Original Revision: https://phabricator.services.mozilla.com/D228217

Phabricator Automation
Updated • 1 year ago

Attachment #9443469 - Flags: approval-mozilla-esr128?

Phabricator Automation
Comment 20 • 1 year ago

esr128 Uplift Approval Request

- **User impact if declined**: An attacker could make Firefox use a different protocol than the one specified in the ALPN header.
- **Code covered by automated testing**: yes
- **Fix verified in Nightly**: yes
- **Needs manual QE test**: yes
- **Steps to reproduce for manual QE testing**: see ~~comment 0~~
- **Risk associated with taking this patch**: medium
- **Explanation of risk level**: Our code coverage for this isn't great. I'm not 100% sure our ALPN negotiation doesn't have any bugs that would cause us to fail loading websites in specific circumstances.
- **String changes made/needed**: none
- **Is Android affected?**: yes

Flags: qe-verify+

Phabricator Automation
Updated • 1 year ago

Attachment #9443469 - Flags: approval-mozilla-esr128? → approval-mozilla-esr128+

Pulsebot
Comment 21 • 1 year ago

uplift

`https://hg.mozilla.org/releases/mozilla-esr128/rev/64544b16dbbb`

Lando Automation
Updated • 1 year ago

status-firefox-esr128: affected → fixed

Valentin Gosu [:valentin] Assignee
Updated • 1 year ago

Flags: ~~needinfo?(valentin.gosu)~~

Bianca Hidecuti, Desktop Test Engineering [:bhidecuti]
Comment 22 • 1 year ago

Verified as fixed on Firefox 128.6.0esr, build ID 20241213173517 (treeherder build from ~~Comment 21~~), using Windows 11, macOS 13.6 and Ubuntu 22.04.

Status: RESOLVED → VERIFIED
status-firefox-esr128: fixed → verified
Flags: ~~qe-verify+~~

Frederik Braun [:freddy]
Updated • 1 year ago

Whiteboard: [client-bounty-form][necko-triaged][necko-priority-queue] → [client-bounty-form][necko-triaged][necko-priority-queue][adv-main134+][adv-ESR128.6+]

Frederik Braun [:freddy]
Comment 23 • 1 year ago

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

Frederik Braun [:freddy]
Updated • 1 year ago

Alias: CVE-2025-0239

Ryan VanderMeulen [:RyanVM]
Updated • 1 year ago

Regressions: ~~1940508~~

Tom Schuster
Updated • 1 year ago

Regressions: ~~1943011~~

Valentin Gosu [:valentin] Assignee
Updated • 1 year ago

See Also: → ~~1943911~~

pspaul Reporter
Comment 24 • 1 year ago

Hey, thanks for taking care of this bug and thanks for the bounty!

I would like to publish a blog post about this bug, is there any embargo period I have to take into account or could I publish it right away?

Thanks!

Frederik Braun [:freddy]
Comment 25 • 1 year ago

This was fixed last release (~4 weeks ago). We generally wait about six weeks to make sure that even users in the more remote parts of the world had the opportunity to upgrade. If possible, I would like you to wait you for another two weeks.

pspaul Reporter
Comment 26 • 1 year ago

Sounds good to me! I'll publish it in two weeks then.

Daniel Veditz [:dveditz]
Updated • 10 months ago

Group: ~~core-security-release~~

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

Top ↑