Copy Summary ▾ View ▾

Closed Bug 1691153 (CVE-2021-23999) Opened 2 years ago Closed 2 years ago

Blob URLs loaded by system principal may be given the incorrect principal

▾ **Categories**

Product:	Core ▾	Type:	defect
Component:	DOM: File ▾	Priority:	P1 Severity: S2

▾ **Tracking**

Status: VERIFIED FIXED
Milestone: 88 Branch

Tracking Flags:

	Tracking	Status
firefox-esr78	88+	fixed
firefox86	---	wontfix
firefox87	---	wontfix
firefox88	---	verified

▸ **People** (Reporter: nika, Assigned: edenchuang)

▸ **References**

▸ **Details** (Keywords: csectype-priv-escalation, sec-moderate, Whiteboard: [post-critsmash-triage] [qa-triaged][adv-main88+][adv-esr78.10+])

▾ **Attachments**

poc Details
2 years ago **Nika Layzell [:nika] (ni? for response)**
175 bytes, text/html

Bug 1691153 - mochitest for testing Blob URL data is transmitted with correct principal type. r=asuth RyanVM : **approval-mozilla-esr78+** Details | Review
2 years ago **Frederik Braun [:freddy]**
48 bytes, text/x-phabricator-request

Bug 1691153 - Using the blob's principal for BlobURLRegistrationData creation in ContentParent::TransmitBlobURLsForPrincipal. r?asuth RyanVM : **approval-mozilla-esr78+** Details | Review
2 years ago **Eden Chuang[:edenchuang]**
48 bytes, text/x-phabricator-request

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

Bottom ↓ Tags ▾ Timeline ▾

Nika Layzell [:nika] (ni? for response) Reporter
Description • 2 years ago

*Attached file **poc** — Details*

STR (from a fresh browser)

1. Load the attached proof of concept. A blob URL will appear in the document, copy it to the clipboard.
2. Open a new tab, paste the blob URL in the address bar, and load it

Expected: The blob should load and display the string `undefined`
Actual: The blob loads and displays the string `[object BrowsingContext]`

Likely Cause

The reason behind this display being different is that the blob URL's document was loaded with the system principal, and thus has privileged access. This is caused by a series of errors in the code which transmits information about Blob URLs to content processes (thanks :asuth for helping me figure out what's going on here!).

1. The code in `ContentParent::TransmitBlobURLsForPrincipal` includes the wrong principal in the `BlobURLRegistrationData` to be sent to the content process. Specifically the registration is created with the principal `aPrincipal` , which is the principal passed to the function, rather than the principal `aBlobPrincipal` which was used to register the blob. (https://searchfox.org/mozilla-central/rev/400614dec36182ba6d0bec2a18044c47df960a1f/dom/ipc/ContentParent.cpp#6123,6137). This means that the wrong principal will be transmitted in cases where these principals don't match.
2. The code uses `aPrincipal->Subsumes(aBlobPrincipal)` instead of `->Equals` , meaning it will pass if `aPrincipal` is an expanded or system principal. This combines with the first issue to mean that if `aPrincipal` is the system principal, a registration will be transmitted with the system principal for all registered Blob URLs (https://searchfox.org/mozilla-central/rev/400614dec36182ba6d0bec2a18044c47df960a1f/dom/ipc/ContentParent.cpp#6126)
3. When ~~bug 1626573~~ was fixed, logic was added to various codepaths which can cause URLs to load from the parent process to try to force blob URLs to be registered in the content process before the load completes. Unfortunately, this code passes `triggeringPrincipal` as the principal to use (https://searchfox.org/mozilla-central/rev/400614dec36182ba6d0bec2a18044c47df960a1f/docshell/base/BrowsingContext.cpp#1847-1848, https://searchfox.org/mozilla-central/rev/400614dec36182ba6d0bec2a18044c47df960a1f/netwerk/ipc/DocumentLoadListener.cpp#1835), which is the system principal in the case where the load is triggered by browser UI (e.g. through pasting a URL in the address bar). This combines with the previous two bugs to cause us to register blob URLs with the wrong (potentially system) principal.

Potential Fix

We should fix all 3 of these core issues in order to make sure we transmit the correct blob URLs with the correct principals. The first issue can be fixed by passing `aBlobPrincipal` instead of `aPrincipal` to the various callsites in the function. The second can be fixed by using `->Equals` instead of `->Subsumes` .

The third bug should be fixed by using the actual principal of the relevant blob URL rather than the triggering principal. This should be doable by removing the `aPrincipal` argument from `TransmitBlobDataIfBlobURL`, and instead implementing it as:

```
nsCOMPtr<nsIPrincipal> blobPrincipal;
if (BlobURLProtocolHandler::GetBlobURLPrincipal(aURI, getter_AddRefs(blobPrincipal))) {
  TransmitBlobURLsForPrincipal(blobPrincipal);
}
```

Exploitability

While this is a serious issue, we are fortunate that it is somewhat tricky to get full system-principal permissions with it. The user has to load the URL in question in a different process than the original page, and the triggering principal must be the system principal (which hopefully requires direct user intervention), such as the user pasting the blob URL into their address bar.

Andrew Sutherland [:asuth] (he/him)
Comment 1 • 2 years ago

I'm going to try and dig into understanding and enumerating the motivating use cases for the blob URL transmission to make sure we don't regress any current blob URL use cases without intent in addressing points 2 and 3. The highest priority is addressing point 1 of the Likely Causes, as that's the core of the problem and principal confusion, so if 2/3 look like they'll take longer, we should likely focus on addressing point 1.

Assignee: nobody → bugmail
Status: NEW → ASSIGNED
Priority: -- → P1

Andrew Sutherland [:asuth] (he/him)
Comment 2 • 2 years ago

Nika provided a pernosco trace on Friday as well: https://pernos.co/debug/U3Q4v_1wxjdpsFmKDDiyYw/index.html

Andrew McCreight [:mccr8]
Updated • 2 years ago

Group: ~~core-security~~

Tom Tung [:tt, :ttung]
Comment 3 • 2 years ago

I am going to set the severity to S2 because the workaround doesn't seem to exist but it requires getting system principal which makes this harder to be exploited.

Andrew, please feel free to adjust the severity if you have different thoughts on this.

Severity: -- → S2

Daniel Veditz [:dveditz]
Updated • 2 years ago

Keywords: csectype-priv-escalation, sec-moderate

Frederik Braun [:freddy]
Comment 5 • 2 years ago

*Attached file **Bug 1691153 - mochitest for testing Blob URL data is transmitted with correct principal type. r=asuth** — Details*

Frederik Braun [:freddy]
Comment 6 • 2 years ago

@asuth: started writing a test because of the dupe. Feel free to steal, when you get to this bug .

Eden Chuang[:edenchuang] Assignee
Updated • 2 years ago

Assignee: bugmail → echuang

Eden Chuang[:edenchuang] Assignee
Comment 7 • 2 years ago

*Attached file **Bug 1691153 - Using the blob's principal for BlobURLRegistrationData creation in ContentParent::TransmitBlobURLsForPrincipal. r?asuth** — Details*

Phabricator Automation
Updated • 2 years ago

Attachment #9206345 - Attachment description: Bug 1691153 - wip test → Bug 1691153 - mochitest for testing Blob URL data is transmitted with correct principal type. r=asuth

Sebastian Hengst [:aryx] (needinfo me if it's about an intermittent or backout)
Comment 8 • 2 years ago

Using the blob's principal for BlobURLRegistrationData creation in ContentParent::TransmitBlobURLsForPrincipal. r=asuth
https://hg.mozilla.org/integration/autoland/rev/18e47349b0f0e1df159db0446cf5706b864a4f15
https://hg.mozilla.org/mozilla-central/rev/18e47349b0f0

Group: dom-core-security → core-security-release
Status: ASSIGNED → RESOLVED
Closed: 2 years ago
status-firefox88: --- → fixed
Resolution: --- → FIXED
Target Milestone: --- → 88 Branch

Eden Chuang[:edenchuang] Assignee
Updated • 2 years ago

Status: RESOLVED → REOPENED

Resolution: FIXED → ---

Release mgmt bot [:suhaib / :marco/ :calixte]
Updated • 2 years ago

status-firefox88: fixed → affected

:Gijs (he/him)
Comment 9 • 2 years ago

Why was this reopened? There's no backout listed, is the fix not working?

Flags: needinfo?(echuang)

Eden Chuang[:edenchuang] Assignee
Comment 10 • 2 years ago

Reopen for landing test.

Flags: ~~needinfo?(echuang)~~

:Gijs (he/him)
Comment 11 • 2 years ago

(In reply to Eden Chuang[:edenchuang] from ~~comment #10~~)

> Reopen for landing test.

But reopening means that the bug's resolution, release tracking fields and target milestone are all wrong, and will make it harder to deal with regressions from this bug, track backouts, track release notes / CVEs, track QA efforts, and so on.

The easier thing to do is either keep the bug closed and just land tests from the closed bug in a few weeks/months time, assuming you don't forget, or file a new security-sensitive bug for the tests and then move the tests to that bug.

Flags: needinfo?(echuang)

Eden Chuang[:edenchuang] Assignee
Comment 12 • 2 years ago

Mark it as resolved-fixed. Keep ni for test landing.

Using the blob's principal for BlobURLRegistrationData creation in ContentParent::TransmitBlobURLsForPrincipal. r=asuth
https://hg.mozilla.org/integration/autoland/rev/18e47349b0f0e1df159db0446cf5706b864a4f15
https://hg.mozilla.org/mozilla-central/rev/18e47349b0f0

Status: REOPENED → RESOLVED
Closed: 2 years ago → 2 years ago
Resolution: --- → FIXED

Eden Chuang[:edenchuang] Assignee
Updated • 2 years ago

status-firefox88: affected → fixed
Flags: ~~needinfo?(echuang)~~

Eden Chuang[:edenchuang] Assignee
Updated • 2 years ago

Flags: needinfo?(echuang)

Sebastian Hengst [:aryx] (needinfo me if it's about an intermittent or backout)
Comment 13 • 2 years ago • Edited

mochitest for testing Blob URL data is transmitted with correct principal type. r=asuth
https://hg.mozilla.org/integration/autoland/rev/bf0c333ee3906ad5fe9a7a86d6dcd390eacb1e39
https://hg.mozilla.org/mozilla-central/rev/bf0c333ee390

Julien Cristau [:jcristau]
Updated • 2 years ago

status-firefox86: --- → wontfix
status-firefox87: --- → wontfix
status-firefox-esr78: --- → ?
Flags: in-testsuite+

Brindusa Tot[:brindusat]
Updated • 2 years ago

Flags: qe-verify+
Whiteboard: [post-critsmash-triage]

Eden Chuang[:edenchuang] Assignee
Updated • 2 years ago

Flags: ~~needinfo?(echuang)~~

Ryan VanderMeulen [:RyanVM]
Comment 14 • 2 years ago

It looks like ESR78 may also be affected by this? If so, we'll probably want a rebased patch and an uplift request please :)

Flags: needinfo?(echuang)

Eden Chuang[:edenchuang] Assignee
Comment 15 • 2 years ago

Sure, will do that.

Flags: ~~needinfo?(echuang)~~

Julien Cristau [:jcristau]
Updated • 2 years ago

status-firefox-esr78: ? → affected
tracking-firefox-esr78: --- → 88+

Eden Chuang[:edenchuang] Assignee
Comment 16 • 2 years ago

Comment on attachment 9207771 [details]
~~Bug 1691153~~ - Using the blob's principal for BlobURLRegistrationData creation in ContentParent::TransmitBlobURLsForPrincipal. r?asuth

ESR Uplift Approval Request

- **If this is not a sec:{high,crit} bug, please state case for ESR consideration**: Blob URLs can be loaded with system principal by a very tricky way.
- **User impact if declined**: A malicious webpage can be loaded with a system principal and hack Firefox.
- **Fix Landed on Version**: 88
- **Risk to taking this patch**: Low
- **Why is the change risky/not risky? (and alternatives if risky)**: The patch is not risky since it just uses the correct principal to load the blob URL.
- **String or UUID changes made by this patch**: No

Attachment #9207771 - Flags: approval-mozilla-esr78?

Eden Chuang[:edenchuang] Assignee
Updated • 2 years ago

Attachment #9206345 - Flags: approval-mozilla-esr78?

Cornel Ionce [:noni] [Hubs QA]
Updated • 2 years ago

Whiteboard: [post-critsmash-triage] → [post-critsmash-triage] [qa-triaged]

Cornel Ionce [:noni] [Hubs QA]
Comment 17 • 2 years ago

Reproduced the initial issue with the attached POC on Firefox 87.0.

Confirming that the expected result is met on Firefox 88.0b5, buildID 20210330185720.

Status: RESOLVED → VERIFIED
status-firefox88: fixed → verified
Flags: ~~qe-verify+~~

Ryan VanderMeulen [:RyanVM]
Comment 18 • 2 years ago

Comment on attachment 9207771 [details]
~~Bug 1691153~~ - Using the blob's principal for BlobURLRegistrationData creation in ContentParent::TransmitBlobURLsForPrincipal. r?asuth

Thanks for rebasing. Approved for 78.10esr.

Attachment #9207771 - Flags: approval-mozilla-esr78? → approval-mozilla-esr78+

Ryan VanderMeulen [:RyanVM]
Updated • 2 years ago

Attachment #9206345 - Flags: approval-mozilla-esr78? → approval-mozilla-esr78+

Ryan VanderMeulen [:RyanVM]
Comment 19 • 2 years ago
uplift

https://hg.mozilla.org/releases/mozilla-esr78/rev/84e39acf7cdf
https://hg.mozilla.org/releases/mozilla-esr78/rev/6bed6549f522

status-firefox-esr78: affected → fixed

Tom Ritter [:tjr]
Updated • 2 years ago

Whiteboard: [post-critsmash-triage] [qa-triaged] → [post-critsmash-triage] [qa-triaged][adv-main88+]

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

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

Andrew Sutherland [:asuth] (he/him)
Comment 21 • 2 years ago

The advisory seems appropriately scoped for the fix that landed (bullet 1 of ~~comment 0~~), thank you. I'll be spinning off bug(s) for points 2 and 3 this week(end).

Tom Ritter [:tjr]
Updated • 2 years ago

Whiteboard: [post-critsmash-triage] [qa-triaged][adv-main88+] → [post-critsmash-triage] [qa-triaged][adv-main88+][adv-esr78.10+]

Frederik Braun [:freddy]
Updated • 2 years ago

Alias: CVE-2021-23999

Andrew Sutherland [:asuth] (he/him)
Comment 22 • 1 year ago

(In reply to Andrew Sutherland [:asuth] (he/him) from ~~comment #21~~)

> The advisory seems appropriately scoped for the fix that landed (bullet 1 of ~~comment 0~~), thank you. I'll be spinning off bug(s) for points 2 and 3 this week(end).

These other bullets ended up getting addressed by ~~bug 1719184~~ which addressed points 2 and 3 by moving the subsumes check to an equals-ish check based on origin hash and ceasing to use the triggering principal as the basis for anything.

Daniel Veditz [:dveditz]
Updated • 1 year ago

Group: ~~core-security-release~~

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

Top ↑