

Copy Summary

View

Closed

Bug 1338637 (CVE-2021-23956)

Opened 6 years ago

Closed 2 years ago

Arbitrary local files disclosure in input[webkitdirectory]

Categories

Product: Core

Component: Widget

Version: 52 Branch

Type: defect

Priority: P2

Severity: normal

Tracking

Status: RESOLVED FIXED

Milestone: 85 Branch

Tracking Flags:

firefox-esr78

firefox85

Tracking

---

---

Status

won't fix

fixed

People

(Reporter: qab, Assigned: pbz)

References

( URL )

Details

(Keywords: csectype-disclosure, sec-moderate, stale-bug, Whiteboard: [adv-main85+])

Attachments

poc.html

6 years ago Abdulrahman Alqabandi

684 bytes, text/html

Details

Bug 1338637 - Ask user for confirmation before folder upload. r=gijs

2 years ago Paul Zühlicke [pbz]

47 bytes, text/x-phabricator-request

Details | Review

Bug 1338637 - Added test for folder upload confirmation prompt. r=gijs

2 years ago Paul Zühlicke [pbz]

47 bytes, text/x-phabricator-request

Details | Review

Bug 1338637 - Updated webkitdirectory test to handle confirm prompts. r=gijs

2 years ago Paul Zühlicke [pbz]

47 bytes, text/x-phabricator-request

Details | Review

advisory.txt

2 years ago Frederik Braun [freddy]

282 bytes, text/plain

Details

Show Obsolete

Bottom

Tags

Timeline

Abdulrahman Alqabandi

Reporter

Description • 6 years ago

Attached file poc.html — Details

User Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36

Steps to reproduce:

Note: This was originally part of ~~Bug 1319370~~ but this turned to be a separate bug deserving of its own report.

1. Open attached PoC

2. Hold down 'enter'

3. If the last used/default folder is 'my documents' (on windows)

4. All the contents of that folder will be accessible without the explicit permission from the user.

( believe it's the case that this works on more folders in non-windows OS

Actual results:

Once a folder upload prompt appears, IFF a user was holding down the 'enter' key the last used directory/default (if they are within 'My Documents' folder or similar) we are able to trick the user into giving us access to all the files in my documents.

Expected results:












The folder upload button should be blurred from.












Abdulrahman Alqabandi

Reporter

Comment 1 • 6 years ago

Could you please test on non-windows Os?

Comment hidden (typo)	+
 <b>Andrea Marchesini [:baku]</b> Comment 3 • 6 years ago	-
On linux the default directory is 'Desktop'. I agree we should not put the focus on the 'OK' button.	
Flags: <a href="#">needinfo?@amarchesini</a>	
 <b>Abdulrahman Alqabandi</b> <span>Reporter</span> Comment 4 • 6 years ago	-
<p>I was thinking about a workaround if this was fixed by simply blurring the button and I think there is still a way to do it.</p> <p>We can theoretically predict where the upload button would appear, with the coordinates at hand we can trick the user into clicking an area on the document repeatedly. After the user is recorded clicking a few times we could insert an input element right where the user is clicking, now since the user is clicking on the coordinates where the upload button will appear, the user could potentially be fooled into pressing the upload file button and disclose all files.</p> <p>So I think the only safe solution here is to completely disable the button and only enable it once a folder has been selected via click or keyboard keys. Alternatively, always default to a un-uploadable pseudo-folder (for a lack of a better word) similar to Windows' "This PC" location. Hope other operating systems have something similar.</p>	
 <b>Al Billings [:abillings - ex-MoCo]</b> Updated • 6 years ago	-
Flags: sec-bounty?	
 <b>Andrew McCreight [:mccr8]</b> Updated • 6 years ago	-
Group: firefox-core-security → core-security Component: Untriaged → DOM Product: Firefox → Core	
 <b>Andrew McCreight [:mccr8]</b> Updated • 6 years ago	-
Group: core-security → dom-core-security	
 <b>Andrew Overholt [:overholt]</b> Updated • 6 years ago	-
Assignee: nobody → amarchesini Priority: -- → P1	
 <b>Andrew Overholt [:overholt]</b> Comment 5 • 6 years ago	-
Andrea, please investigate a fix. Thanks.	
 <b>Daniel Veditz [:dveditz]</b> Updated • 6 years ago	-
Keywords: <a href="#">csectype-disclosure</a> , <a href="#">sec-moderate</a>	
 <b>Andrew McCreight [:mccr8]</b> Comment 6 • 6 years ago	-
It looks like this has been posted publicly in <a href="http://leucosite.com/Chrome-Firefox-Edge-Local-File-Disclosure/">http://leucosite.com/Chrome-Firefox-Edge-Local-File-Disclosure/</a>	
URL: <a href="http://leucosite.com/Chrome-Firefox-E...">http://leucosite.com/Chrome-Firefox-E...</a>	
Comment hidden (off-topic)	+
 <b>Al Billings [:abillings - ex-MoCo]</b> Updated • 6 years ago	-
Flags: sec-bounty? → sec-bounty-	
Comment hidden (off-topic)	+
 <b>Abdulrahman Alqabandi</b> <span>Reporter</span> Comment 9 • 6 years ago	-
<p>(In reply to Al Billings [:abillings] from <a href="#">comment #8</a>)</p> <ul style="list-style-type: none"> <li>&gt; Abdulrahman, if it isn't clear. Publicly discussing the details of a</li> <li>&gt; security bug that we haven't fixed yet is bad form, especially if you never</li> <li>&gt; put any disclosure date warnings in communications with us. 90 days, at</li> <li>&gt; least, is the industry standard for people that do put such guidelines on</li> <li>&gt; disclosure into place. Finding out via twitter and blogs that you've</li> <li>&gt; potentially 0dayed users is not cool.</li> </ul> <p>I don't think this bug is as severe given <a href="#">Bug-1319370</a> was fixed, the chances of this affecting any Nightly users is low in my opinion, especially since I disclosed publicly. I definitely should have re-read the bug bounty policy, last I read it it mentioned giving at least 60 days for bugs to be fixed, this was removed. Keep in mind I reported this in <a href="#">Bug-1319370</a> 5 months ago and its been reported here 2 months ago (the 60 I assumed</p>	

was minimum), so I hope you see I did not have any bad intent just looked like to me I had the right to publicly disclose given everything. Also, I had reported this to Google 8 months and I was eager to write about it.		
I will be sure to give you guys a heads up if I ever intend on doing something like this again now that I re-read the policy. Apologies for any inconvenience.		
Comment hidden (off-topic)		+
Comment hidden (off-topic)		+
Comment hidden (off-topic)		+
 <b>Andrea Marchesini [:baku]</b> Comment 13 • 6 years ago		-
The bug is not in DOM. we should implement something better at a FilePicker widget level.		
Component: DOM → Widget		
 <b>Emma Humphries</b> 🌈 🏳️‍🌈 🏳️‍🌈 (she/they) [:emceeai] (Pacific Time) use needinfo Comment 14 • 5 years ago		-
This is an assigned P1 bug without activity in two weeks.		
If you intend to continue working on this bug for the current release/iteration/sprint, remove the 'stale-bug' keyword.		
Otherwise we'll reset the priority of the bug back to '-' on Monday, August 28th.		
Keywords: <a href="#">stale-bug</a>		
 <b>Andrea Marchesini [:baku]</b> Updated • 5 years ago		-
Assignee: amarchesini → nobody		
 <b>Andrea Marchesini [:baku]</b> Comment 15 • 5 years ago		-
Somebody working on widgets should take it.		
 <b>Andrew McCreight [:mccr8]</b> Comment 16 • 5 years ago		-
Jim, do you know who might be able to work on this?		
Flags: needinfo?(jmathies)		
 <b>Jim Mathies [:jimm]</b> Updated • 5 years ago		-
Flags: <a href="#">needinfo?(jmathies)</a> Priority: P1 → P2		
 <b>Jim Mathies [:jimm]</b> Comment 17 • 5 years ago		-
I can reproduce. My default was desktop so nothing happened. I think the idea that the user must hold the enter button (triggering repeat) makes this a bit of an outlier. Will find an owner.		
Status: UNCONFIRMED → NEW Ever confirmed: true		
 <b>:Gijs (he/him)</b> Comment 19 • 5 years ago		-
So unsurprisingly, "some people" are now reporting dupes based on the publicized stuff from qab (also pinned tweet...) as gone over in previous comments. I think we should assume people will try to exploit this if/when convenient to them given it's all public at this point.		
Jim, can you please find someone to own this?		
Flags: needinfo?(jmathies)		
 <b>Abdulrahman Alqabandi</b> <span>Reporter</span> Comment 20 • 5 years ago		-
I am still ashamed for that. My apologies for making things more complicated. FWIW I unpinnd the tweet. Also, Chrome went with showing a dialog before files are uploaded (along with removing focus from OK button in some OS).		
 <b>Jim Mathies [:jimm]</b> Updated • 5 years ago		-
Flags: <a href="#">needinfo?(jmathies)</a>		
 <b>Daniel Veditz [:dveditz]</b> Comment 21 • 5 years ago		-

This is bad UI that could be improved to reduce the opportunities for social engineering, but it does not meet the severity level for the Bug Bounty program.

Group: ~~dom-core-security~~  
Flags: sec-bounty? → sec-bounty-



**:Gijs (he/him)**  
Comment 23 • 2 years ago



Looks like on Windows you can require interaction with the view in the modal dialog before the OK button is enabled by passing `FOS_OKBUTTONNEEDSINTERACTION` (which is listed as one of the relevant options on the doc site, but with no explanation, so I wonder when that got added and on what OSes it's supported...). That seems to wfm on win10.

However, even Edge does not appear to use it; it instead prompts for confirmation before uploading, as does Chrome - with a dialog that then defaults to `[Cancel]` (despite the styling of the dialog buttons suggesting that "Upload" is the default, which is... weird.)

Dan, what do you think about doing the same?

Flags: needinfo?(dveditz)



**:Gijs (he/him)**  
Updated • 2 years ago



Flags: needinfo?(gijskruitbosch+bugs)



**:Gijs (he/him)**  
Comment 25 • 2 years ago



Paul, do you have cycles to look at adding a confirmation dialog using the tab-modal dialog infrastructure to mimic Edge/Chrome? Looks like somewhere like <https://searchfox.org/mozilla-central/rev/e1d1f043957191616721b9e8bf811c0aab8a203a/dom/html/HTMLInputElement.cpp#483> would work?

Flags: needinfo?(gijskruitbosch+bugs) → needinfo?(pbz)



**Paul Zühlcke [:pbz]** Assignee  
Updated • 2 years ago



Assignee: nobody → pbz  
Status: NEW → ASSIGNED  
Flags: needinfo?(pbz)



**Paul Zühlcke [:pbz]** Assignee  
Comment 26 • 2 years ago



Attached file [Bug 1338637 - Ask user for confirmation before folder upload. r=gijs](#) — Details



**Paul Zühlcke [:pbz]** Assignee  
Comment 27 • 2 years ago



Attached file [Bug 1338637 - Added test for folder upload confirmation prompt. r=gijs](#) — Details

This also fixes an issue where MockFilePicker wouldn't set the mode correctly, which caused it to always use "modeOpen". For this test we need to pass "modeGetFolder" in order for the prompt to show.

Depends on D95324



**Pulsebot**  
Comment 28 • 2 years ago



Pushed by [pzuhlcke@mozilla.com](mailto:pzuhlcke@mozilla.com):  
<https://hg.mozilla.org/integration/autoland/rev/5c29fd30af97>  
Ask user for confirmation before folder upload. r=Gijs,geckoview-reviewers,agi,baku  
<https://hg.mozilla.org/integration/autoland/rev/5bddcb99f650>  
Added test for folder upload confirmation prompt. r=Gijs



**Razvan Maries**  
Comment 29 • 2 years ago



Backed out for perma failures.

Push with failure: [https://treeherder.mozilla.org/jobs?repo=autoland&selectedTaskRun=LMOCGoNbT1Kf1udXtFq\\_Nw.0&resultStatus=testfailed%2Cbusted%2Cexception&revision=5bddcb99f650063907888fe944ac6c3cc7e7ba69](https://treeherder.mozilla.org/jobs?repo=autoland&selectedTaskRun=LMOCGoNbT1Kf1udXtFq_Nw.0&resultStatus=testfailed%2Cbusted%2Cexception&revision=5bddcb99f650063907888fe944ac6c3cc7e7ba69)

Log: [https://treeherder.mozilla.org/logviewer?job\\_id=321917169&repo=autoland&lineNumber=5103](https://treeherder.mozilla.org/logviewer?job_id=321917169&repo=autoland&lineNumber=5103)

Backout: <https://hg.mozilla.org/integration/autoland/rev/72c8c0774cee0aac6084838f837186f904f7bb52>

Flags: needinfo?(pbz)



**Paul Zühlcke [:pbz]** Assignee  
Comment 30 • 2 years ago



Attached file [Bug 1338637 - Updated webkitdirectory test to handle confirm prompts. r=gijs](#) — Details

Depends on D96526



**Pulsebot**  
Comment 31 • 2 years ago



Pushed by [pzuhlcke@mozilla.com](mailto:pzuhlcke@mozilla.com):  
<https://hg.mozilla.org/integration/autoland/rev/fa598dea0903>  
Ask user for confirmation before folder upload. r=Gijs,geckoview-reviewers,baku  
<https://hg.mozilla.org/integration/autoland/rev/9515d8916527>

Added test for folder upload confirmation prompt. r=Gijs  
<https://hg.mozilla.org/integration/autoland/rev/7b898a8dac3c>  
Updated webkitdirectory test to handle confirm prompts. r=Gijs



**Paul Zühlcke** [pbz] Assignee  
Updated • 2 years ago



Flags: ~~needinfo?~~(pbz)



**Sebastian Hengst** [aryx] (needinfo me if it's about an intermittent or backout)  
Comment 32 • 2 years ago



bugherder

<https://hg.mozilla.org/mozilla-central/rev/fa598dea0903>  
<https://hg.mozilla.org/mozilla-central/rev/9515d8916527>  
<https://hg.mozilla.org/mozilla-central/rev/7b898a8dac3c>

Status: ASSIGNED → RESOLVED  
Closed: 2 years ago  
[status-firefox85: --- → fixed](#)  
Resolution: --- → FIXED  
Target Milestone: --- → 85 Branch



**Paul Zühlcke** [pbz] Assignee  
Updated • 2 years ago



Blocks: [1628586](#)



**Frederik Braun** [fredr] Assignee  
Updated • 2 years ago



Whiteboard: [adv-main85+]



**Frederik Braun** [fredr] Assignee  
Comment 33 • 2 years ago



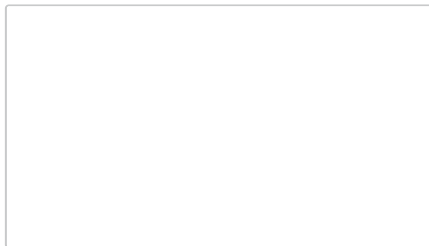
Attached file [advisory.txt](#) (obsolete) — [Details](#)



**Frederik Braun** [fredr] Assignee  
Comment 34 • 2 years ago



Attached file [advisory.txt](#) — [Details](#)



Attachment #9198097 - Attachment is obsolete: true



**Frederik Braun** [fredr] Assignee  
Updated • 2 years ago



Alias: CVE-2021-2395



**Frederik Braun** [fredr] Assignee  
Updated • 2 years ago



Alias: CVE-2021-2395 → CVE-2021-23956



**Tom Ritter** [tjr] Assignee  
Updated • 2 years ago



Flags: sec-bounty-hof+



**Daniel Veditz** [dveditz] Assignee  
Updated • 2 years ago



Flags: ~~needinfo?~~(dveditz)



**Daniel Veditz** [dveditz] Assignee  
Updated • 2 years ago



[status-firefox-esr78: --- → affected](#)



**Ryan VanderMeulen** [RyanVM] Assignee  
Updated • 1 year ago



[status-firefox-esr78: affected → wontfix](#)

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