

XSS vulnerability in CologneBlue (CVE-2020-29002)

Closed, ResolvedPublicSECURITY

Actions

Assigned To

matmarex

Authored By

Jdlrobson
2020-11-04 22:57:23 (UTC+0)

Tags

Security-Team (Our Part Is Done)

Security

Vuln-XSS

CologneBlue (Backlog)

MW-1.36-notes (1.36.0-wmf.14; 2020-10-20)

MW-1.35-notes

Referenced Files

F32438524: 0001-Fix-escaping-of-the-qbfind-message.patch

2020-11-05 18:33:13 (UTC+0)

Subscribers

Aklapper

Ammarpad

Daimona

DannyS712

Jdlrobson

matmarex

Reedy

View All 9 Subscribers

Description

this was flagged by @Daimona on the review of https://gerrit.wikimedia.org/r/c/mediawiki/skins/CologneBlue/+637771/2/includes/CologneBlueTemplate.php#395

Set the qbfind message to:

"<script>alert(0);</script>Findz";

Cologne blue will alert 0.

This happens in current master and was only flagged(noticing) during adjustments to the code.

Details

Author Affiliation

WMF Product

Project	Subject
mediawiki/skins/CologneBlue	SECURITY: Fix escaping of the 'qbfind' message
mediawiki/skins/CologneBlue	SECURITY: Fix escaping of the 'qbfind' message
mediawiki/skins/CologneBlue	SECURITY: Fix escaping of the 'qbfind' message
mediawiki/skins/CologneBlue	SECURITY: Fix escaping of the 'qbfind' message
mediawiki/skins/CologneBlue	SECURITY: Fix escaping of the 'qbfind' message
mediawiki/skins/CologneBlue	SECURITY: Fix escaping of the 'qbfind' message
mediawiki/skins/CologneBlue	SECURITY: Fix escaping of the 'qbfind' message
mediawiki/skins/CologneBlue	SECURITY: Fix escaping of the 'qbfind' message

Customize query in gerrit

Related Objects

Mentions

Mentioned In

T263040: Write and send supplementary release announcement for extensions and skins with security patches (1.31.11/1.35.4)

Mentioned Here

T263040: Write and send supplementary release announcement for extensions and skins with security patches (1.31.11/1.35.4)
T2212: Some MediaWiki: messages not safe in HTML (tracking)



Daimona added a comment.

2020-11-04 22:58:07 (UTC+0)

Urgh, I'm sorry. I didn't realize master was already affected.

Jdlrobson updated the task description. (Show Details)

2020-11-04 23:13:53 (UTC+0)

Jdlrobson added a subscriber: Ammarpad.

Urbanecm triaged this task as High priority.

2020-11-05 01:16:30 (UTC+0)

Urbanecm added projects: Vuln-XSS, CologneBlue.

Urbanecm added subscribers: matmarex, Danny5712.

Urbanecm added a subscriber: Urbanecm.

matmarex added a comment.

2020-11-05 18:28:34 (UTC+0)

I don't think this needs to be a security task. This is a system message, and so it's only vulnerable to administrators. We have a public tracking task for issues like this (T2212). We should just submit a patch to Gerrit and merge it.

matmarex added a comment.

2020-11-05 18:33:13 (UTC+0)

Let me know if I shouldn't just submit the patch to Gerrit. Otherwise I'll do it tomorrow.

0001-Fix-escaping-of-the-qbfind-message.patch

862 B

Download

Daimona added a comment.

2020-11-05 18:38:16 (UTC+0)

In T267278#660707+, @matmarex wrote:

I don't think this needs to be a security task. This is a system message, and so it's only vulnerable to administrators. We have a public tracking task for issues like this (T2212). We should just submit a patch to Gerrit and merge it.

That's true, although I can remember of some similar tasks being kept sec-protected and assigned a CVE recently. Just because exploiting is presumably hard (but who knows, perhaps there's a workaround to being administrators), it's still a possible attack vector: you only need to compromise a sysop account, which is likely much easier than compromising an IA account. So I'd be paranoid and keep it protected. As for the fix, I guess it can be pushed on gerrit as long as someone is around to sec-deploy it.

Either way, I'm obviously leaving this up to the SecTeam (and approving your patch, just in case).

sbassett added a subscriber: sbassett.

Edited · 2020-11-05 18:38:43 (UTC+0)

In T267278#6607088, @matmarex wrote:

Let me know if I shouldn't just submit the patch to Gerrit. Otherwise I'll do it tomorrow.

+1 to the patch above and this is low risk to go to gerrit IMO, as the issue was already publicly-flagged in gerrit and I'm not seeing anything remotely suspicious within any of the existing messages after a quick audit.

Jdlrobson added a comment.

2020-11-05 18:40:13 (UTC+0)

Great. I'm happy to merge this Bartosz if you want to throw it up onto Gerrit!

sbassett added a comment.

Edited · 2020-11-05 18:43:47 (UTC+0)

In T267278#6607104, @Daimona wrote:

That's true, although I can remember of some similar tasks being kept sec-protected and assigned a CVE recently.

Yes, I'll likely track this for the upcoming supplemental security announcement (T263810), though since the skin is no longer bundled, once the patch is merged and deployed, this task can be made public and then any relevant backports can be completed. This probably does warrant a CVE as it's still a viable XSS under certain circumstances, so I'll likely eventually request one.

Just because exploiting is presumably hard (but who knows, perhaps there's a workaround to being administrators), it's still a possible attack vector: you only need to compromise a sysop account, which is likely much easier than compromising an IA account. So I'd be paranoid and keep it protected. As for the fix, I guess it can be pushed on gerrit as long as someone is around to sec-deploy it.

Yes, agreed. I'm hopeful the merge/deploy can happen quickly. If not, I'm happy to sec-deploy it once the patch is merged.

sbassett mentioned this in T263810: Write and send supplementary release announcement for extensions and skins with security patches (1.31.11/1.35.1).

2020-11-05 18:49:22 (UTC+0)

sbassett added a project: Patch-For-Review.

2020-11-05 20:14:02 (UTC+0)

Ok, the patch is up for review (@Jdlrobson et al):
<https://gerrit.wikimedia.org/r/639618>
If we could get this reviewed and merged soon, that'd be great.

Jdforrester-WMF added projects: MW-1.36-notes (1.36.0-wmf.14, 2020-10-20), MW-1.35-notes.

2020-11-07 00:50:50 (UTC+0)

sbassett lowered the priority of this task from High to Low.

2020-11-09 16:35:15 (UTC+0)

sbassett moved this task from Incoming to Watching on the Security-Team board.

sbassett added a subscriber: Reedy.

This fix was deployed to production (1, 2, tx @Reedy !). I'm tracking this task for the next supplemental release: T263810. So we can likely make this task public soon and work on any relevant backports and requesting the CVE.

sbassett changed the visibility from "Custom Policy" to "Public (No Login Required)".

2020-11-09 22:29:31 (UTC+0)

gerritbot added a comment.

2020-11-09 22:29:47 (UTC+0)

Change 640194 had a related patch set uploaded (by SBassett; owner: Bartosz Dziewoński):
[mediawiki/skins/CologneBlue@REL1_34] SECURITY: Fix escaping of the 'qbfind' message

<https://gerrit.wikimedia.org/r/640194>

 **gerritbot** added a comment. 2020-11-09 22:30:36 (UTC+0)


Change 640195 had a related patch set uploaded (by SBassett; owner: Bartosz Dziewoński):
[mediawiki/skins/CologneBlue@REL1_31] SECURITY: Fix escaping of the 'qbfind' message

<https://gerrit.wikimedia.org/r/640195>

 **gerritbot** added a comment. 2020-11-09 22:44:11 (UTC+0)


Change 640194 **merged** by jenkins-bot:
[mediawiki/skins/CologneBlue@REL1_34] SECURITY: Fix escaping of the 'qbfind' message

<https://gerrit.wikimedia.org/r/640194>


 **gerritbot** added a comment. 2020-11-10 20:36:18 (UTC+0)


Change 640195 **merged** by SBassett:
[mediawiki/skins/CologneBlue@REL1_31] SECURITY: Fix escaping of the 'qbfind' message


<https://gerrit.wikimedia.org/r/640195>

 **sbassett** renamed this task from *XSS vulnerability in CologneBlue* to *XSS vulnerability in CologneBlue (CVE-2020-29002)*. 2020-12-01 17:45:10 (UTC+0)

 **sbassett** closed this task as *Resolved*. 2020-12-01 17:54:52 (UTC+0)

 **sbassett** assigned this task to **matmarex**.

 **sbassett** moved this task from *Watching* to *Our Part Is Done* on the **Security-Team** board.

 **sbassett** removed a project: **Patch-For-Review**.