lists.wikimedia.org allows unsubscribing other users without prior confirmation (CVE-2021-40347)

Closed, Resolved · Public · SECURITY

Actions

Assigned To
Legoktm

Authored By
PleaseStand
2021-08-26 17:02:12 (UTC+0)

Tags
Security
Wikimedia-Mailing-lists (Backlog)
SecTeam-Processed (Completed)
Upstream (Patch merged upstream)
SRE (Backlog)

Referenced Files
None

Subscribers
Aklapper
Ladsgroup
Legoktm
PleaseStand
sbassett

Tokens

Description

Step-by-step instructions to reproduce the issue (in Firefox web browser):

1. Select two different email addresses (A and B) for which you can receive messages. Aliases are OK; you do not need to send any message from either email account in order to reproduce the issue.
2. If already logged in to lists.wikimedia.org, log out now.
3. Go to https://lists.wikimedia.org/postorius/lists/mediawiki-announce.lists.wikimedia.org/
4. Subscribe using email address A (creating an account doesn't matter) and confirm the request as instructed.
5. If already logged in to lists.wikimedia.org, log out now.
6. Go to https://lists.wikimedia.org/accounts/signup/
7. Create an account using email address B and confirm the request as instructed.
8. Go to https://lists.wikimedia.org/accounts/login/?next=/postorius/lists/mediawiki-announce.lists.wikimedia.org/ (if prompted to log in, do so using the account associated with email address B)
9. Right-click on the drop-down list (selected option should be "Primary Address") and select "Inspect".
10. Set the name attribute of the select element to "email".
11. Set the value attribute of the first option element to email address A.
12. In the action value of the form element, replace "subscribe" with "unsubscribe/" (including the forward slash at the end).
13. Click the "Subscribe" button.
14. Check the inbox for email address A.

Note that in addition to user A being unsubscribed, user B receives positive confirmation that user A was subscribed to the mailing list in question, in a way not subject to Wikimedia's IP rate limit on anonymous subscriptions through the web interface. If user A were not subscribed, user B would get the error, "a@example.com is not a member address of mediawiki-announce@lists.wikimedia.org".

OWASP vulnerability category: A5:2017-Broken Access Control

Details

Author Affiliation
Wikimedia Communities

Related Objects

Mentions

Mentioned In
~~T289099: Security Review For Mailman3 / lists.wikimedia.org~~

PleaseStand created this task. 2021-08-26 17:02:12 (UTC+0)

Restricted Application added a subscriber: **Aklapper**. · View Herald Transcript 2021-08-26 17:02:13 (UTC+0)

Ladsgroup added a project: **Wikimedia-Mailing-lists**. 2021-08-26 17:07:22 (UTC+0)

Ladsgroup added a subscriber: **Ladsgroup**. 2021-08-26 17:09:57 (UTC+0)

Legoktm added a subscriber: **Legoktm**. 2021-08-26 17:16:09 (UTC+0)

Thanks for the fantastic report @PleaseStand, I'll start looking into this now. Just to clarify, have you already reached out to the Mailman security team about this? If not that's fine, I'll do that once I figure out what's going wrong...

PleaseStand added a comment. 2021-08-26 17:18:06 (UTC+0)

> In ~~T289798#7312668~~, **@Legoktm** wrote:

> *Thanks for the fantastic report* **@PleaseStand** *, I'll start looking into this now. Just to clarify, have you already reached out to the Mailman security team about this? If not that's fine, I'll do that once I figure out what's going wrong...*

No, I have not yet checked whether this bug has already been fixed by the Mailman developers.

sbassett edited projects, added **SecTeam-Processed**; removed **Security-Team**. 2021-08-26 17:29:32 (UTC+0)

sbassett added a subscriber: **sbassett**.

When I test, I notice that I *do* receive an error when I try to subscribe an email address which is already subscribed. But that appears not to matter for this attack?

Legoktm added a comment. Edited · 2021-08-26 18:46:05 (UTC+0)

The vulnerable code is https://gitlab.com/mailman/postorius/-/blob/master/src/postorius/views/list.py#L553 (the version we have deployed is the same, but without the self._has_pending_unsub_req check)

Here's my proposed patch:

```
diff --git a/src/postorius/views/list.py b/src/postorius/views/list.py
index f03f1c13..1864c71f 100644
--- a/src/postorius/views/list.py
+++ b/src/postorius/views/list.py
@@ -553,6 +553,15 @@ class ListUnsubscribeView(MailingListView):
     @method_decorator(login_required)
     def post(self, request, *args, **kwargs):
         email = request.POST['email']
+        # Verify the user actually controls this email
+        user_emails = EmailAddress.objects.filter(
+            user=request.user, verified=True).order_by(
+            "email").values_list("email", flat=True)
+        if email not in user_emails:
+            messages.error(
+                request,
+                _('You can only unsubscribe yourself.'))
+            return redirect('list_summary', self.mailing_list.list_id)
         if self._has_pending_unsub_req(email):
             messages.error(
                 request,
```

For simplicity, I copied the user_emails part out of ListSubscribeView earlier in that file. I've live-hacked this to https://polymorphic.lists.wmcloud.org/postorius/lists/ and tested it there (note that test6 has unsubscribe approval enabled, so you can't actually unsubscribe people on that list). Verified that I could no longer unsubscribe other people, but I could still unsubscribe myself.

@Ladsgroup want to take a quick look at this patch before I put it on lists1001?

And then I'll do a quick audit of the other endpoints before sending a report upstream.

Legoktm claimed this task. 2021-08-26 22:20:45 (UTC+0)

Legoktm triaged this task as *Medium* priority.

Deployed the above patch to lists.wikimedia.org: https://sal.toolforge.org/log/ptx_hHsBa_6PSCT9tXB4 and verified that trying to unsubscribe an address gets the "You can only unsubscribe yourself" error.

I skimmed the other endpoints in postorius/views/list.py and they seemed fine, most have `@list_owner_required` style decorators that I assume work properly.

Legoktm added a project: **Upstream**. 2021-08-26 22:37:27 (UTC+0)

Reported upstream: https://gitlab.com/mailman/postorius/-/issues/531, also going to poke their mailing list.

Legoktm added a comment. 2021-08-26 22:39:42 (UTC+0)

Oh, **@PleaseStand** , how would you prefer to be credited in the report and CVE? Username, real name, both?

Legoktm moved this task from **Backlog** to **Reported Upstream** on the **Upstream** board. 2021-08-26 22:45:34 (UTC+0)

Platonides awarded a token. 2021-08-26 22:46:20 (UTC+0)

Jdforrester-WMF awarded a token. 2021-08-26 23:04:21 (UTC+0)

PleaseStand added a comment. 2021-08-27 00:19:43 (UTC+0)

> In ~~T289798#7313559~~, **@Legoktm** wrote:
> *Oh,* **@PleaseStand** *, how would you prefer to be credited in the report and CVE? Username, real name, both?*

Kevin Israel (Wikipedia user PleaseStand)

Legoktm renamed this task from *lists.wikimedia.org allows unsubscribing other users without prior confirmation* to *lists.wikimedia.org allows unsubscribing other users without prior confirmation (CVE-2021-40347)*. 2021-08-31 22:19:01 (UTC+0)

Legoktm added a comment. 2021-09-01 07:25:08 (UTC+0)

My patch has been merged upstream: https://gitlab.com/mailman/postorius/-/commit/3d880c56b58bc26b32eac0799407d74b64b7474b so I'll update our package in the next few days and deploy it properly. I also sent a note to the Debian security team.

Legoktm moved this task from **Reported Upstream** to **Patch merged upstream** on the **Upstream** board. 2021-09-01 07:25:22 (UTC+0)

Legoktm closed this task as *Resolved*. 2021-09-07 15:29:07 (UTC+0)

Upstream released 1.3.5 with the fix.

Legoktm changed the visibility from "**Custom Policy**" to "Public (No Login Required)". 2021-09-07 15:29:22 (UTC+0)

Legoktm changed the edit policy from "**Custom Policy**" to "All Users".

Maintenance_bot added a project: **SRE**. 2021-09-07 15:45:21 (UTC+0)

Legoktm added a comment. 2021-09-09 18:49:25 (UTC+0)

DSA issued: https://lists.debian.org/debian-security-announce/2021/msg00155.html

Legoktm mentioned this in **~~T289899: Security Review For Mailman3 / lists.wikimedia.org~~**. 2021-10-14 17:57:05 (UTC+0)