Closed · Issue created 1 year ago by legoktm

Logged-in user can unsubscribe anyone from any list using specially crafted POST request (CVE-2021-40347)

I'm forwarding this security report from Kevin Israel (Wikipedia user PleaseStand), who discovered this on lists.wikimedia.org and filed a reporti n our tracker: https://phabricator.wikimedia.org/T289798. Using a specially crafted POST request, a logged-in user can unsubscribe anyone from any list.

Reproduction steps:

1. Subscribe to a mailing list with address A and confirm the subscription
2. Create an account using address B, and visit a mailing list page that you are not subscribed to, you should see the subscription form and an address dropdown.
3. Using your browsers inspector, change the form's URL by replacing `subscribe` with `unsubscribe/`
4. Change the `name` attribute on the address `<select>` to "email".
5. Change the value of the selected option to be address A.
6. Click the "Subscribe" button.

You'll see that address A has now been unsubscribed. Additionally, address B now knows that A was subscribed to the list, allowing for leaking the subscriber list as they'd receive an error like ""a@example.com is not a member address of ..." if A was not subscribed.

The cause is https://gitlab.com/mailman/postorius/-/blob/master/src/postorius/views/list.py#L553, which does not verify the user owns the email address being unsubscribed.

Here's a patch that I've tested works functionally and deployed to lists.wikimedia.org:

```
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,
```

I copied the user_emails chunk from earlier in this file to make sure I didn't implement the query wrong. If that looks good I can add the news entry, etc. and submit a MR - let me know.

Edited 1 year ago by legoktm

Drag your designs here or click to upload.

Tasks 0

No tasks are currently assigned. Use tasks to break down this issue into smaller parts.

Linked items 0

Link issues together to show that they're related or that one is blocking others. Learn more.

Related merge requests 1

Check a user owns the email they are trying to unsubscribe (CVE-2021-40347)
!657

When this merge request is accepted, this issue will be closed automatically.

Activity

legoktm changed the description 1 year ago

Abhilash Raj @maxking · 1 year ago — Owner

Thanks for the report @legoktm, this definitely looks like a bug.

How about just writing a query to see if there is a record with `email` and `request.user` in the database? We can avoid fetching all emails and doing comparison in Python in that case?

Also, lets start an MR with the change. I'd like to get this into a security release and see if I can backport the MR to the current stable release. We'd probably want to release the patch as well, since we need to patch this in older versions of Postorius.

I need to look up how many previous versions of P are affected by this, perhaps using git-blame.

Edited by Abhilash Raj 1 year ago

legoktm @legoktm · 1 year ago — Author, Contributor

> How about just writing a query to see if there is a record with `email` and `request.user` in the database? We can avoid fetching all emails and doing comparison in Python in that case?

Is this what you had in mind?

```
        found_email = EmailAddress.objects.filter(
            user=request.user, email=email, verified=True).count()
        if found_email == 0:
            messages.error(
                request,
                _('You can only unsubscribe yourself.'))
            return redirect('list_summary', self.mailing_list.list_id)
```

> Also, lets start an MR with the change.

Will do in a moment. The CVE request is pending, hopefully I'll have it tomorrow.

> I need to look up how many previous versions of P are affected by this, perhaps using git-blame.

It's been present ever since 1.0.0, I didn't look past that: https://gitlab.com/mailman/postorius/-/blob/1.0.0/src/postorius/views/list.py#L293

legoktm mentioned in merge request !657 (merged) 1 year ago

legoktm @legoktm · 1 year ago — Author, Contributor

MR submitted: !657 (merged)

Abhilash Raj @maxking · 1 year ago — Owner

I did not realize it but creating an MR makes the bug public :(

Abhilash Raj @maxking · 1 year ago — Owner

Thanks for the MR @legoktm, we'd need a test for it but other than that, it looks good to me.

legoktm changed title from **Logged-in user can unsubscribe anyone from any list using specially crafted POST request** to **Logged-in user can unsubscribe anyone from any list using specially crafted POST request (CVE-2021-40347)** 1 year ago

legoktm @legoktm · 1 year ago — Author, Contributor

@maxking added some tests, and updated the MR with the now-assigned CVE.

> I did not realize it but creating an MR makes the bug public :(

Oh, I thought that's what you had intended for, sorry. I don't have any option to delete it, not sure if you do.

Abhilash Raj closed via commit 7494e880 1 year ago

legoktm closed via commit 3d880c56 1 year ago

Abhilash Raj @maxking · 1 year ago

Owner

I did want to, but I forgot to mention this feature for creating a confidential merge request from the the confidential issue https://docs.gitlab.com/12.10/ee/user/project/issues/confidential_issues.html#merge-requests-for-confidential-issues

I guess it'd be better to do that or co-ordinate over patches.

Thanks for your help with the patch though, you've been very helpful and your contributions are much appreciated!

legoktm mentioned in commit 0de3cdcd 1 year ago

legoktm @legoktm · 1 year ago

Author Contributor

@maxking, can you make this issue public now? Thanks

Abhilash Raj made the issue visible to everyone 1 year ago