Talos Vulnerability Report

TALOS-2020-1178

phpGACL return_page redirection open redirect vulnerability

JANUARY 27, 2021

CVE NUMBER

CVE-2020-13565

Summary

An open redirect vulnerability exists in the return_page redirection functionality of phpGACL 3.3.7. A specially crafted HTTP request can redirect users to an arbitrary URL. An attacker can provide a crafted URL to trigger this vulnerability.

Tested Versions

OpenEMR 5.0.2
OpenEMR development version 6.0.0 (commit babec93f600ff1394f91ccd512bcad85832eb6ce)
phpGACL 3.3.7

Product URLs

http://phpgacl.sourceforge.net/

CVSSv3 Score

6.1 - CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

CWE

CWE-601 - URL Redirection to Untrusted Site ('Open Redirect')

Details

phpGACL is a PHP library that allows developers to implement permission systems via a Generic Access Control List.

The latest version of this library has been found to be used in OpenEMR, as such the tests have been performed against an OpenEMR instance.

The file `gacl_admin_api.class.php` (in OpenEMR this has been renamed to `Gacl/GaclAdminApi.php`) defines a `return_page` function that is supposed to be used to redirect an admin user to a specified page:

```
function return_page($url="") {
    global $_SERVER, $debug;

    if (empty($url) AND !empty($_SERVER[HTTP_REFERER])) {
        $this->debug_text("return_page(): URL not set, using referer!");
        $url = $_SERVER[HTTP_REFERER];
    }

    if (!$debug OR $debug==0) {
        header("Location: $url\n\n");             [1]
    } else {
        $this->debug_text("return_page(): URL: $url -- Referer: $_SERVER[HTTP_REFERRER]");
    }
}
```

At [1] we can see that the `$url` passed as argument is used in the location header without any sanitization.

As an example, one instance where this function is used is in `admin/acl_list.php`:

```
...
switch ($_GET['action']) {
    case 'Delete':
        $gacl_api->debug_text('Delete!');

        if (is_array ($_GET['delete_acl']) AND !empty($_GET['delete_acl'])) {
            foreach($_GET['delete_acl'] as $id) {
                $gacl_api->del_acl($id);
            }
        }

        //Return page.
        $gacl_api->return_page($_GET['return_page']);   [2]
        break;
...
```

The `return_page` variable is controllable the query string [2], meaning that an attacker could supply a malicious link to the phpGACL instance, which eventually will redirect the user to an arbitrary location controlled by the attacker. This can be abused to conduct phishing attacks and steal credentials.

Additionally, the `return_page` function should either call `exit()` or `die()` before returning, otherwise execution would continue, which could result in unexpected behavior.

Exploit Proof of Concept

The issue above has been reproduced by testing against OpenEMR, which ships the latest version of phpGACL.

An attacker could send the following link to an admin user to reproduce:

```
http://open-erm.dev/gacl/admin/acl_list.php?action=Delete&return_page=http://open-emr.org&site=default
```

Clicking on this link will redirect the user to an arbitrary page (in this example “http://open-emr.org”).

Timeline

2020-10-21 - Vendor Disclosure
2021-01-05 - Vendor Patched
2021-01-27 - Public Release

CREDIT

Discovered by Claudio Bozzato of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT
TALOS-2020-1174

NEXT REPORT
TALOS-2020-1177