tkostalSBA and lxp Publish SBA-ADV-20220328-01: Vtiger CRM Sto... ... on Sep 27 History

..

README.md 2 months ago

README.md

Vtiger CRM Stored Cross-Site Scripting

Vulnerability Overview

Vtiger CRM 7.4.0 or below is prone to a stored cross-site scripting vulnerability in the email templates module due to insufficient sanitizing.

- **Identifier** : SBA-ADV-20220328-01
- **Type of Vulnerability** : Cross Site Scripting
- **Software/Product Name** : Vtiger CRM
- **Vendor** : Vtiger
- **Affected Versions** : <= 7.4.0
- **Fixed in Version** : Not yet
- **CVE ID** : CVE-2022-38335
- **CVSS Vector** : CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N
- **CVSS Base Score** : 7.6 (High)

Vendor Description

> Vtiger is a PHP based web application that enables businesses to increase sales wins, marketing ROI, and support satisfaction by providing tools for employees and management work more effectively, capture more data, and derive new actionable insights from across the customer lifecycle.

Source: https://code.vtiger.com/vtiger/vtigercrm

Impact

An authenticated attacker with the "Email Templates"-module privilege is able to insert JavaScript into email templates, which is triggered when a victim views the template. In the worst case, the victim's session could be hijacked and the attacker is able to perform actions in the victim's context. This could lead to privilege escalation if the victim is more privileged than the attacker (for example an admin).

Vulnerability Description

The following code snippet (`./modules/Emails/models/Mailer.php`) shows the function which should ensure that JavaScript is removed from the user input:

```
[...]
public static function getProcessedContent($content) {
    // remove script tags from whole html content
    $processedContent = preg_replace('#<script(.*?)>(.*?)</script>#is', '', $content
$processedContent = purifyHtmlEventAttributes($processedContent,TRUE);
    return $processedContent;
}
[...]
```

However, the regex `#<script(.*?)>(.*?)</script>#is` is insufficient for sanitizing JavaScript.

Proof of Concept

If the attacker inserts the payload `<script>alert(1)</script` into an email template, the JavaScript code will not be removed, because the regex does not work due to the missing `>`. The following request demonstrates saving a template containing the malicious payload:

```
POST /index.php HTTP/1.1
Host: example.org
Cookie: PHPSESSID=[...]
[...]

__vtrftk=[...]&module=EmailTemplates&action=Save&record=16&subject=Invitation&system
```

To load the content of the corresponding template, the following request is sent by the victim:

```
POST /index.php HTTP/1.1
Host: example.org
Cookie: PHPSESSID=[...]
[...]

__vtrftk=[...]&module=EmailTemplates&action=ShowTemplateContent&mode=getContent&reco
```

The server responds with the content that contains the injected JavaScript:

```
HTTP/1.1 200 OK
[...]

{"success":true,"result":{"content":"<html>\r\n<head>\r\n\t<title><\/title>\r\n<\/he
```

After that, the HTML content is inserted into the iframe with the id `TemplateIFrame`, where the JavaScript is executed within the victim's browser.

Recommended Countermeasures

We are not aware of a vendor fix yet. Please contact the vendor.

In other places of the source code, in addition to the `purifyHtmlEventAttributes` function, the `purify` function of the class `HTMLPurifier` is used to sanitize JavaScript. The function `getProcessedContent` should also use `HTMLPurifier` instead of the regex.

Timeline

- `2022-03-28` : identified the vulnerability in version 7.4.0
- `2022-03-28` : initial vendor contact through public address
- `2022-03-28` : disclosed vulnerability to vendor
- `2022-04-14` : vendor will look into vulnerability
- `2022-05-30` : contacted vendor again but received no reply
- `2022-08-12` : request CVE from MITRE
- `2022-09-16` : MITRE assigned CVE-2022-38335
- `2022-09-27` : public disclosure

References

- Vtiger CRM 7.4.0: https://code.vtiger.com/vtiger/vtigercrm/repository/archive.zip?ref=7.4.0GA

Credits

- Corinna Rudlstorfer (SBA Research)
- Thomas Kostal (SBA Research)
- Jakob Pachmann (SBA Research)