Security advisory

Multiple SQL injection in AzurWebEngine (AzurCMS) <= 1.2.3.12

June, 2021

CVE-2021-27950
Release date: 30/06/2021
Department: POST Cyberforce
Roman Zakharov
Jean-Marie Bourbon

Vulnerability summary

Product	AzurWebEngine in AzurCMS
Product homepage	https://www.sitasoftware.lu/web.php
Affected product versions	1.2.3.12 and earlier
Severity	Critical: CVSS v3.1 score - 9.2
CVSS v3.1	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:F/RL:O
MITRE ATT&CK	T1190, T1606, T1505.003
OWASP	OWASP 2017-A1
CWE	CWE-89
Workarounds	No workarounds available
Fixed product versions	1.2.4.3 or request a hotfix from Vendor

Validated impact:

- Unautorized access;
- Admin/User accounts takeover;
- Remote code execution.

Timeline

Date	Action
24 February 2021	Vulnerability identification, exploitation and impact validation
25 February 2021	Vendor notified and acknowledged the vulnerability
02 March 2021	Vendor advised on mitigation actions
04 March 2021	CVE-2021-27950 assigned by MITRE
05 March 2021	Vendor informed about assigned CVE id
24 March 2021	Request for updates
29 March 2021	Received the update from Vendor
12 May 2021	Received the update from Vendor
30 June 2021	Advisory publicly released by POST Cyberforce

References:

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27950
- https://attack.mitre.org/techniques/T1190/
- https://attack.mitre.org/techniques/T1606/
- https://attack.mitre.org/techniques/T1505/003/
- https://owasp.org/www-project-top-ten/2017/A1_2017-Injection
- https://cwe.mitre.org/data/definitions/89.html

Product description

Azur Web Engine is part of Azur CMS which is a website Content Management System. It includes several modules such as:

- Azur ticket: A ticket system is an administration module allowing the implementation of a project and the oversight of its progress by level of importance.
- Calendar: The calendar allows syncing between team members.
- Time management: Time management is Azur WEB's time management module.
- Intranet: Intranet is a module made exclusively for internal activities.
- Control center: Control Center is the module made for tracking your company's financial results in real-time.

Azur CMS includes an E-business module, which turns the website into an Online store.

Advisory

During the penetration test POST Cyberforce identified multiple SQL injection vulnerabilities in AzurWebEngine within Sita AzurCMS including 1.2.3.12, which allows an attacker to execute arbitrary SQL commands.

Injection points require authentication as a simple online shop user. The account creation process is simple and does not require any additional validation from the website owner's side.

Any website guest or legitimate user, who performs online shopping actions, could leverage SQL injection to gain unauthorized access, obtain sensitive information, conduct administrator account takeover attacks and execute the code remotely.

Vulnerability description

The application executes SQL queries containing user-supplied input without proper server-side validation. This allows an attacker to send specially crafted input and modify SQL queries without proper server-side validation. In the identified endpoint two actions present - **`docdl`** and **`docdetail`**.

Both actions require authentication, however, anybody can create an account to proceed with online purchases. **`docdl`** action generates a PDF file on every request what makes the exploitation slower. **`docdetail`** action does not generate a PDF file on every request. The **`id`** parameter is vulnerable to SQL injection.

Database user privilege is system administrator (sysdba) which opens an attacker unlimited access to all databases hosted on this SQL server.

The most interesting data lies in the USERS table, where an attacker found Azur CMS administrators account data including not hashed **`password reset token`**. Using a **`password reset token`** it is possible to change an administrator account password, login into Azur CMS admin panel, achieve Remote Code Execution and revert the password. Azur CMS admin panel allows an attacker to change PHP files meaning that any part of the application could be used to have persistent access to the affected website.

`Vulnerable endpoints:`

GET /mesdocs.ajax.php?action=docdl&id=XXX&no_fiche=XXX HTTP/1.1

GET /mesdocs.ajax.php?action=docdetail&id=XXX HTTP/1.1

`Vulnerable parameter:` id

Proof of concept

GET /mesdocs.ajax.php?action=docdl&id=3%20order+by+1&no_fiche=130 HTTP/1.1

GET /mesdocs.ajax.php?action=docdetail&id=2%20AND%201%3d1 HTTP/1.1

Recommendation

Contact Sita Software S.A. to receive an updated version.