Back to all zero days

CVE-2021-33853 - Stored Cross-Site Scripting in X2CRM

AFFECTED VENDOR	STATUS	DATE
X2CRM	Fixed	Dec 1, 2021

Description Proof of concept (POC) Impact Remediations Timeline

Description

A Cross-Site Scripting (XSS) attack can cause arbitrary code (javascript) to run in a user's browser while the browser is connected to a trusted website. As the vehicle for the attack, the application targets the users and not the application itself. Additionally, the XSS payload is executed when the user attempts to access any page of the CRM.

Affected Vendor
X2CRM

Bug Name
Stored Cross-Site Scripting

CVE Number
CVE-2021-33853

CWE ID
CWE-79

CSW ID
2021-CSW-11-1054

CVSSv3 Score
6.1

Affected Version
Version 8.0

Severity
Medium

Affected Product
X2CRM

Proof of concept: (POC)

The following vulnerability was discovered in X2CRM version 8.0.

Issue: Stored Cross-Site Scripting

1. Login to the X2CRM as administrator.
2. Go to the "Administrator" tool and click on the "User Interface Management" submenu and select "Add Top Bar Link".

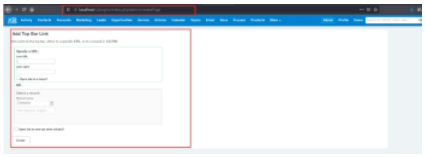

Figure 1: Add Top Bar Page

3. Enter "<script>alert("XSS")</script>" in the "Link Name" field and submit the request.

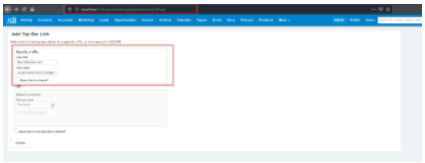

Figure 2: Payload injected in "Link Name" field

4. By accessing any page within the CRM, the payload will be executed.

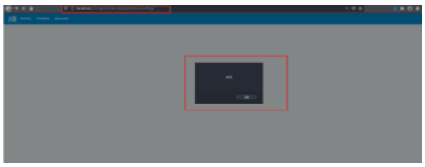

Figure 3: XSS Payload Triggered

Impact

An attacker can perform the following -

- Inject malicious code into the vulnerable variable and exploit the application through the Cross-Site Scripting vulnerability.
- Modify the code and get the session information of other users.
- Compromise the user machine.

Remediations

- Perform context-sensitive encoding of entrusted input before echoing back to a browser using an encoding library throughout the application.
- Implement input validation for special characters on all the variables are reflected in the browser and stored in the database.
- Explicitly set the character set encoding for each page generated by the webserver.
- Encode dynamic output elements and filter specific characters in dynamic elements.

Timeline

November 11, 2021: Discovered in X2CRM 8.0` Product

December 1, 2021: CSW team reported to Vendor about the vulnerability.

January 20, 2022: X2CRM team postponed the release of X2CRM 8.5.

2021-33853).

Talk to CSW's team of experts to secure your landscape.

Schedule free consultation

Cyber Security Works helps reduce security debt and inherent vulnerabilities in an organization's infrastructure and code. We work with large public, private, and start-up companies and help them prioritize their vulnerabilities.

Resources

- Ransomware
- Cyber Risk Series
- Blogs
- Patch Watch
- Data Sheets
- White Papers
- Zero Days
- Glossary
- Events
- CISA-KEV

Partner

- Become a Partner

Quick Links

- About Us
- Contact Us
- Careers
- Services
- Media Coverage
- Cybersecurity month
- Predictions for 2022
- Cybersecurity for govt
- Hackathon