

Stored Cross-Site Scripting (XSS) Vulnerability - (EQWebClient)

000045918 | Reference | Last updated 2026-09-02 | ControlSuite, ControlSuite Equitrac

Issue

Stored Cross-Site Scripting (XSS) Vulnerability

Cause

Stored Cross-Site Scripting (XSS) is a type of security vulnerability that occurs when a malicious script is permanently stored on a target server, such as in a database, comment field, or forum post. When other users access the affected page, the malicious script is executed in their browsers, allowing attackers to steal sensitive information, hijack user sessions, or perform other malicious actions

Solution

The Tungsten development team has implemented a fix to mitigate the Stored XSS vulnerability. The fix includes the following measures:

Input Validation and Sanitization:

All user inputs are treated as untrusted and are validated and sanitized before being stored in the database. This ensures that malicious scripts cannot be injected into the application

To request this fix, please open a technical support case

Applies to

Product	Version
ControlSuite	2025.2

<https://aio-eus-uat-cae-aif-app14-local.redglacier-35d7ee4f.eastus.azurecontainerapps.io/article/45918>