Vulnerability Summary

CVE #	CVE-2023-26599
Description	XSS vulnerability in Triplesign in Tripleplay Platform releases prior to Caveman 3.4.0 allows attackers to inject client side code to run as an authenticated user via a crafted link
Affected Versions	All Tripleplay releases before Caveman 3.4.0
Date	24/02/2023
Severity	Medium - CVSS 6.5 (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L)

Summary

It is possible, by getting a user to click on a carefully crafted link, for an attacker to inject JavaScript code into the management pages which is executed in the users browser. This could enable them to extract information from the system and make changes to some of the configuration or content on the system depending on the users' privileges.

On a fully patched, up-to-date system it would not be possible to modify user accounts credentials or create new user accounts using this vulnerability.

Mitigations

There are no methods to mitigate the attack, so it is recommended that users immediately move to remediation.

Remediation

All remediation options require package installation by a trained Uniguest Support Engineer or Technical Services Engineer. Please contact your technical account representative or email support@tripleplay.tv to arrange an upgrade.

Recommended Remediation:

- Upgrade to Caveman 3.4, or a later release, which includes the fix for this issue as well as many other OS level security fixes

Alternate Remediation:

- For systems running Caveman 3.2.0 install patch-TPS-3493-triplesign-content-reflected-xss-caveman-3.2.0-1.0.0.99114.T.tar.bz2
- For system running releases prior to Caveman 3.2.0 upgrade to one of the above releases and install the patch