tripleplay
by uniguest

Vulnerability Summary

CVE #	CVE-2023-25760
Description	Incorrect Access Control in Tripleplay Platform releases prior to Caveman 3.4.0 allows authenticated user to modify other users passwords via a crafted request payload
Affected Versions	All Tripleplay releases before Caveman 3.4.0
Date	17/02/2023
Severity	High - CVSS 8.0 (CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

Summary

It is possible, through a carefully crafted request payload, for a user, with credentials to access the Tripleplay management pages, to modify the password of a different user. This would enable them to modify the admin user’s password and gain administrative privileges to the Tripleplay Management pages and effectively lock other users out.

This vulnerability is only possible to exploit if the system is not configured to use an external authentication system, such as LDAP/AD or SAML.

Mitigations

Configure the Tripleplay Management system to use an external LDAP, Active Directory or SAML system for authentication through the System Config application.

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 2.3.1 to 3.3.1 install patch-TPS-3400-user-password-change-caveman-3.2.0-1.0.0.98755.T.tar.bz2
- For system running releases prior to Caveman 2.3.1 upgrade to one of the above releases and install the patch