# Vulnerability Summary

| | |
|---|---|
| **CVE #** | CVE-2023-25759 |
| **Description** | OS Command Injection in TripleData Reporting Engine in Tripleplay Platform releases prior to Caveman 3.4.0 allows authenticated users to run unprivileged OS level commands via a crafted request payload |
| **Affected Versions** | All Tripleplay releases before Caveman 3.4.0 |
| **Date** | 17/02/2023 |
| **Severity** | High - CVSS 8.4 (CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:C/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 execute commands at the OS level as an unprivileged system user. This unprivileged user is not able to access files owned by the superuser so the attacker would not be able to read or modify the encrypted password of system accounts and would not be able to modify any of the code running on the Tripleplay server. However, they would be able to read data stored in the file system or database of the Tripleplay products and be able to change configuration options of the Tripleplay platform.

## 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 3.0.0 to 3.3.1 install patch-TPS-3387-tripledata-runreport-shell-exec-caveman-3.2.0-1.0.0.98680.T.tar.bz2
- For systems running Caveman 2.3.1 install patch-TPS-3387-tripledata-runreport-shell-exec-caveman-2.3.1-1.0.0.98756.T.tar.bz2
- For system running releases prior to Caveman 2.3.1 upgrade to one of the above releases and install the appropriate patch