Vulnerability Summary

CVE #	CVE-2024-50706
Description	The vulnerability is triggered when an attacker sends a specially crafted HTTP POST request. The input is not properly sanitized, resulting in the execution of arbitrary SQL commands on the backend database. This SQL injection vulnerability could allow an attacker to access, modify, or delete sensitive data.
Affected Versions	Only affects Tripleplay 23.1+
Date	04/16/2025
Severity	Critical 10.0 - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Acknowledgments

We thank the security researcher(s) who identified and responsibly disclosed this vulnerability.

CVE-2024-50706	Alwin Warringa

Summary

An unauthenticated SQL injection vulnerability exists allowing attackers to execute arbitrary SQL queries on the backend database. This vulnerability is critical and can be exploited remotely without authentication.

Mitigations

A patch to resolve this issue has been released in versions Tripleplay 24.2.1 and 24.1.2. Users are advised to upgrade to these versions as soon as possible. Additionally, patches are available for earlier versions.

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:

- A patch addressing this issue has been released in Tripleplay 24.1.2 and 24.2.1. Users are strongly encouraged to update to this version immediately.