Vulnerability Summary

CVE #	CVE-2024-50707
Description	The vulnerability resides in the handling of the X-Forwarded-For header in HTTP GET requests. By injecting a malicious payload into the header, an attacker can exploit this flaw to execute arbitrary commands on the server. The issue stems from improper input validation and insufficient sanitization of user-supplied header data.
Affected Versions	All Tripleplay releases before 24.2.1
Date	XX/XX/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-2024-50707	Alwin Warringa

Summary

A vulnerability has been identified that allows unauthenticated remote code execution via a specially crafted HTTP GET request. This issue poses an risk as it could allow attackers to execute arbitrary code on the affected system without prior 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:

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.

Alternate Remediation:

-