# Security Update Release Notes

| | |
|---|---|
| **Product:** | Cloud SaaS Platform |
| **Release Version:** | 2024.6.14 |
| **Release Date:** | 2024-06-14 |
| **Status:** | Released |

## Overview

This update addresses multiple security vulnerabilities and strengthens the overall security posture of Cloud SaaS services.

## Resolved Vulnerabilities

- **CVE-2024-XXXX:** Resolved an authentication bypass issue in the user session management module.
- **CVE-2024-YYYY:** Addressed a cross-site scripting (XSS) vulnerability affecting the admin dashboard.
- **Internal Reference #12345:** Fixed improper input validation in the API gateway.

## Enhancements

- Improved password storage by migrating to stronger hashing algorithms.
- Updated third-party libraries and dependencies to latest stable versions.

## Affected Components

1. User Authentication Service
2. Admin Dashboard
3. Public API Endpoints

## Mitigations & Recommendations

- Review your integrations for any custom authentication logic.
- Encourage users to reset passwords if suspicious activity is detected.
- Refer to `docs/security-updates` for implementation guidance.

## Further Information

For more details or support, contact our security team at