OSSTech OpenAM 9.5.5

リリースノート

OSSTech(株)

更新日: 2023 年 4 月 3 日

目次

1. はじめに

本ドキュメントは、OSSTech 提供の OpenAM の修正内容について記載しています。本ドキュメントの対象となる OpenAM パッケージは、osstech-openam-9.5.5-51 です。

このパッケージは ForgeRock コミュニティ版 OpenAM 9.5.5 のソースコードをベースとしています。コミュニティ版のリリースノートについては次のページより確認してください。

https://wikis.forgerock.org/confluence/display/openam/OpenAM+9.5.5+Release+Notes

また、ご利用の OpenAM パッケージのバージョンの確認は次のコマンドで確認することができます。

```
$ rpm -qa | grep osstech-openam
osstech-openam-9.5.5-51.el6.noarch
```

2. osstech-openam-9.5.5-51 の修正内容

OSSTech 提供の OpenAM 9.5.5-51 では以下の修正を行いました。

2.1 9.5.6／11.0.0 以降に統合されている修正(バックポート)

- アクセス制御の不備の脆弱性を修正
  - https://github.com/openam-jp/openam/issues/283

2.2 OSSTech 独自の修正

2.2.1 機能追加

なし

2.2.2 設定関連の変更

なし

2.2.3 問題の修正

- Apache Commons FileUpload の脆弱性 (CVE-2023-24998) によるサービス運用妨害 (DoS) の脆弱性を修正

3. コミュニティ版との差異

OSSTech 提供の OpenAM 9.5.5 は ForgeRock コミュニティ版 OpenAM9.5.5 と以下の差異があります。

3.1 9.5.6／11.0.0 以降に統合されている修正(バックポート)

- カスタム応答プロバイダが無視される問題を修正
  - https://bugster.forgerock.org/jira/browse/OPENAM-333
- SP initiated SSO の場合にユーザーが認証したレルムとトラストサークルのレルムが一致しているかどうかチェックされない問題を修正
  - https://bugster.forgerock.org/jira/browse/OPENAM-77
- WAR ファイルにユニットテスト用の JSP／JAR ファイルが含まれる問題を修正
  - https://bugster.forgerock.org/jira/browse/OPENAM-528
- ポリシー名に UTF-8 が使えない問題を修正
  - https://bugster.forgerock.org/jira/browse/OPENAM-995
- HTTP ヘッダに付加される OpenAM のバージョン情報をデフォルトで無効化するように修正
  - https://bugster.forgerock.org/jira/browse/OPENAM-751
- デフォルトサーバー設定を変更する際に画面にエラーが表示される問題を修正
  - https://bugster.forgerock.org/jira/browse/OPENAM-1896
- IDP アダプタに関して ClassNotFoundException のログが出力される問題の修正
  - https://bugster.forgerock.org/jira/browse/OPENAM-1315
- iPlanetDirectoryPro と AMAuthCookie が同じ値となる問題の修正
  - https://bugster.forgerock.org/jira/browse/OPENAM-75
- 各 JDBC データストアが個別に持つべき設定を共有している問題の修正
  - https://bugster.forgerock.org/jira/browse/OPENAM-1054
- セッションタイムアウト状態でログアウトした場合に goto パラメータが無視される問題を修正
  - https://bugster.forgerock.org/jira/browse/OPENAM-2426
- HTTP-POST バインディングで複数回 AuthnRequest を OpenAM が受け取った場合に認証エラーとなる問題を修正
  - https://bugster.forgerock.org/jira/browse/OPENAM-1858

- JDK のバージョンにより SAML 連携が動作しない問題を修正
  - https://bugster.forgerock.org/jira/browse/OPENAM-2644
- OpenAM を冗長構成としている場合に ClientSDK や ssoadm が動作しない問題を修正
  - https://bugster.forgerock.org/jira/browse/OPENAM-3528
- OpenAM を冗長構成としている場合に Cookie に HttpOnly が付加されない問題を修正
  - https://bugster.forgerock.org/jira/browse/OPENAM-3740
- Secure Attribute Exchange (SAE) 用エンドポイントの XSS 脆弱性の修正
- SAML メタデータをコンソールからインポートする際に失敗する不具合の修正
  - https://bugster.forgerock.org/jira/browse/OPENAM-3005
- SAML フェデレーション時に RelayState パラメータが欠落する不具合の修正
  - https://bugster.forgerock.org/jira/browse/OPENAM-3202
- 特定の状況でシングルログアウトした際にに RelayState パラメータの検証に失敗する不具合の修正
  - https://bugster.forgerock.org/jira/browse/OPENAM-3437
- セキュリティ脆弱性の修正(AM20150408-1)
  - http://www.osstech.co.jp/support/AM20150408-1
- セッション数制限を有効にした状態で ForceAuth を有効にした場合に NullPointerException が発生する問題の修正
  - https://bugster.forgerock.org/jira/browse/OPENAM-6245
- OpenAM のログローテーション機能が実際のログサイズではなく OpenAM が出力したログサイズで実行される問題の修正
  - https://bugster.forgerock.org/jira/browse/OPENAM-4072
- パスワードリセットオプション画面を表示できない問題の修正
  - https://bugster.forgerock.org/jira/browse/OPENAM-2612
- セキュリティ脆弱性の修正(AM20150915-1)
  - http://www.osstech.co.jp/support/AM20150915-1
- セキュリティ脆弱性の修正(AM20160308-1)
  - http://www.osstech.co.jp/support/AM20160308-1
- セキュリティ脆弱性の修正(AM20160726-1)
  - http://www.osstech.co.jp/support/AM20160726-1

- セキュリティ脆弱性の修正(AM20160907-1)
  - http://www.osstech.co.jp/support/AM20160907-1
- セキュリティ脆弱性の修正(AM20161109-1)
  - http://www.osstech.co.jp/support/AM20161109-1
- アクセス制御の不備の脆弱性を修正
  - https://github.com/openam-jp/openam/issues/283

3.2 OSSTech 独自の修正

- Java6 によるビルド時に XSLT エラーが発生する問題の修正
  - https://bugster.forgerock.org/jira/browse/OPENAM-128
- データストアに OpenLDAP 用の設定を追加
- ログアウト時にエラーが発生する問題を修正
- クッキーエンコードの設定の初期値を false から true に変更
- フェデレーションのシークエンスでフォワード先の URL からコンテキスト名までを削除するように修正
- ログインエラー時の画面のリンクに不要な SAML リクエストが含まれる問題を修正
- 画面の文字化けを修正
- 証明書認証モジュールのログ出力のレベルを修正
- CRL 取得処理の不具合を修正
- マルチサーバーモードでのユーザー毎のセッション数チェックの有効化
- データストア認証モジュールにユーザー名文字列の検証処理を追加
- セッションフォワーディングの DoS 脆弱性の修正
- CDCServlet で TARGET パラメーターが重複する問題の修正
- Apache Commons FileUpload におけるサービス運用妨害 (DoS) の脆弱性を修正（CVE-2016-3092）
  - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3092
- SAML の認証コンテキストクラスの問題を修正
- セキュリティ脆弱性の修正(AM20190722-1)
  - https://www.osstech.co.jp/support/am2019-2-1
- OpenAM が発行する Cookie に SameSite=None を付与するオプションを追加

- リモートコード実行の脆弱性(CVE-2021-35464)を修正
- SAML における XML インジェクションの脆弱性を修正
- アクセス制御の不備の脆弱性を修正
  - https://www.osstech.co.jp/support/am2021-7-1/
- Apache Commons FileUpload の脆弱性 (CVE-2023-24998) によるサービス運用妨害 (DoS) の脆弱性を修正

4. 制限事項

- 異なるバージョンの OpenAM を同一の OpenAM サイトに利用することはできません
- データストアのデータベースリポジトリは試験的実装であり本稼働環境での利用を推奨しておりません

5. パッケージ更新履歴

- 2023 年 4 月 3 日 osstech-openam-9.5.5-51
  - アクセス制御の不備の脆弱性を修正
  - Apache Commons FileUpload の脆弱性 (CVE-2023-24998) によるサービス運用妨害 (DoS) の脆弱性を修正
- 2021 年 12 月 23 日 osstech-openam-9.5.5-49
  - アクセス制御の不備の脆弱性を修正
- 2021 年 8 月 23 日 osstech-openam-9.5.5-48
  - SAML における XML インジェクションの脆弱性を修正
- 2021 年 8 月 5 日 osstech-openam-9.5.5-47
  - リモートコード実行の脆弱性(CVE-2021-35464)を修正
- 2020 年 1 月 20 日 osstech-openam-9.5.5-46
  - OpenAM が発行する Cookie に SameSite=None を付与するオプションを追加
- 2019 年 7 月 8 日 osstech-openam-9.5.5-44
  - セキュリティ脆弱性の修正(AM20190722-1)
    - https://www.osstech.co.jp/support/am2019-2-1
- 2017 年 7 月 12 日 osstech-openam-9.5.5-42
  - SAML の認証コンテキストクラスの問題を修正
- 2016 年 11 月 9 日 osstech-openam-9.5.5-41
  - セキュリティ脆弱性の修正(AM20161109-1)
    - http://www.osstech.co.jp/support/AM20161109-1
- 2016 年 9 月 7 日 osstech-openam-9.5.5-40
  - セキュリティ脆弱性の修正(AM20160907-1)
    - http://www.osstech.co.jp/support/AM20160907-1
- 2016 年 7 月 26 日 osstech-openam-9.5.5-37
  - セキュリティ脆弱性の修正(AM20160726-1)
    - http://www.osstech.co.jp/support/AM20160726-1

- Apache Commons FileUpload におけるサービス運用妨害 (DoS) の脆弱性を修正（CVE-2016-3092）
  - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3092

- 2016 年 3 月 8 日 osstech-openam-9.5.5-31
  - セキュリティ脆弱性の修正(AM20160308-1)
    - http://www.osstech.co.jp/support/AM20160308-1

- 2015 年 9 月 15 日 osstech-openam-9.5.5-30
  - セッション数制限を有効にした状態で ForceAuth を有効にした場合に NullPointerException が発生する問題の修正
    - https://bugster.forgerock.org/jira/browse/OPENAM-6245
  - OpenAM のログローテーション機能が実際のログサイズではなく OpenAM が出力したログサイズで実行される問題の修正
    - https://bugster.forgerock.org/jira/browse/OPENAM-4072
  - パスワードリセットオプション画面を表示できない問題の修正
    - https://bugster.forgerock.org/jira/browse/OPENAM-2612
  - セキュリティ脆弱性の修正(AM20150915-1)
    - http://www.osstech.co.jp/support/AM20150915-1

- 2015 年 4 月 8 日 osstech-openam-9.5.5-21
  - セキュリティ脆弱性の修正(AM20150408-1)
    - http://www.osstech.co.jp/support/AM20150408-1
  - CDCServlet で TARGET パラメーターが重複する問題の修正

- 2014 年 11 月 6 日 osstech-openam-9.5.5-16
  - セッションフォワーディングの DoS 脆弱性の修正
  - Secure Attribute Exchange (SAE) 用エンドポイントの XSS 脆弱性の修正
  - SAML メタデータをコンソールからインポートする際に失敗する不具合の修正
    - https://bugster.forgerock.org/jira/browse/OPENAM-3005
  - SAML フェデレーション時に RelayState パラメータが欠落する不具合の修正
    - https://bugster.forgerock.org/jira/browse/OPENAM-3202
  - 特定の状況でシングルログアウトした際にに RelayState パラメータの検証に失敗する不具合の修正

        - https://bugster.forgerock.org/jira/browse/OPENAM-3437
- 2014 年 7 月 22 日 osstech-openam-9.5.5-14
    - セッションタイムアウト状態でログアウトした場合に goto パラメータが無視される問題を修正
        - https://bugster.forgerock.org/jira/browse/OPENAM-2426
    - HTTP-POST バインディングで複数回 AuthnRequest を OpenAM が受け取った場合に認証エラーとなる問題を修正
        - https://bugster.forgerock.org/jira/browse/OPENAM-1858
    - JDK のバージョンにより SAML 連携が動作しない問題を修正
        - https://bugster.forgerock.org/jira/browse/OPENAM-2644
    - OpenAM を冗長構成としている場合に ClientSDK や ssoadm が動作しない問題を修正
        - https://bugster.forgerock.org/jira/browse/OPENAM-3528
    - OpenAM を冗長構成としている場合に Cookie に HttpOnly が付加されない問題を修正
        - https://bugster.forgerock.org/jira/browse/OPENAM-3740
- 2013 年 7 月 1 日 osstech-openam-9.5.5-8
    - 各 JDBC データストアが個別に持つべき設定を共有している問題の修正
        - https://bugster.forgerock.org/jira/browse/OPENAM-1054
- 2013 年 5 月 24 日 osstech-openam-9.5.5-7
    - iPlanetDirectoryPro と AMAuthCookie が同じ値となる問題の修正
        - https://bugster.forgerock.org/jira/browse/OPENAM-75
    - IDP アダプタに関して ClassNotFoundException のログが出力される問題の修正
        - https://bugster.forgerock.org/jira/browse/OPENAM-1315
    - HTTP ヘッダに付加される OpenAM のバージョン情報をデフォルトで無効化するように修正
        - https://bugster.forgerock.org/jira/browse/OPENAM-751
    - デフォルトサーバー設定を変更する際に画面にエラーが表示される問題を修正
        - https://bugster.forgerock.org/jira/browse/OPENAM-1896
- 2012 年 12 月 20 日 osstech-openam-9.5.5-3
    - ポリシー名に UTF-8 が使えない問題を修正
        - https://bugster.forgerock.org/jira/browse/OPENAM-995
- 2012 年 11 月 29 日 osstech-openam-9.5.5-2

- OpenAM 9.5.5 へのバージョンアップ
  - https://wikis.forgerock.org/confluence/display/openam/OpenAM+9.5.5+Release+Notes
- WAR ファイルにユニットテスト用の JSP／JAR ファイルが含まれる問題を修正
  - https://bugster.forgerock.org/jira/browse/OPENAM-528

- 2012 年 11 月 8 日 osstech-openam-9.5.4_RTM-5
  - SP initiated SSO の場合にユーザーが認証したレルムとトラストサークルのレルムが一致しているかどうかチェックされない問題を修正
    - https://bugster.forgerock.org/jira/browse/OPENAM-77
  - goto URL にスラッシュから始まる相対 URL を指定できるように修正
  - データストア認証モジュールにユーザー名文字列の検証処理を追加
  - マルチサーバーモードでのユーザー毎のセッション数チェックの有効化
- 2012 年 2 月 17 日 osstech-openam-9.5.4_RTM-0
  - OpenAM 9.5.4_RTM へのバージョンアップ
    - https://wikis.forgerock.org/confluence/display/openam/OpenAM+9.5.4+Release+Notes
- 2012 年 1 月 24 日 osstech-openam-9.5.3_RTM-3
  - OpenAM 9.5.3_RTM へのバージョンアップ
    - https://wikis.forgerock.org/confluence/display/openam/OpenAM+9.5.3+Release+Notes
  - CRL 取得処理の不具合を修正
  - 証明書認証モジュールのログ出力のレベルを修正
  - osstech-openam-tools パッケージを追加
  - 証明書認証モジュールで OCSP の検証に失敗する問題を修正
    - https://bugster.forgerock.org/jira/browse/OPENAM-586
  - 画面の文字化けを修正
  - カスタム応答プロバイダが無視される問題を修正
    - https://bugster.forgerock.org/jira/browse/OPENAM-333
- 2011 年 8 月 4 日 osstech-openam-9.5.1_RTM-5
  - ログインエラー時の画面のリンクに不要な SAML リクエストが含まれる問題を修正

- フェデレーションのシークエンスでフォワード先の URL からコンテキスト名までを削除するように変更
- amAuthentication.error ログが作成されない問題を修正
  - https://bugster.forgerock.org/jira/browse/OPENAM-502

- 2010 年 12 月 24 日 osstech-openam-9.5.1_RTM-0
  - OpenAM 9.5.1_RTM
  - ログアウト時にエラーが発生する問題を修正
  - クッキーエンコードの設定の初期値を false から true に変更
  - データストアに OpenLDAP 用の設定を追加
  - Java6 によるビルド時に XSLT エラーが発生する問題の修正
    - https://bugster.forgerock.org/jira/browse/OPENAM-128