NOTICE

お知らせ

Apache HTTP Server（mod_http2）の脆弱性への対応のお知らせ

Apache の HTTP/2 モジュールに深刻な脆弱性が公表されました。
速やかに Apache のバージョンアップをお願いいたします。
すぐにできない場合は、HTTP/2 の無効化でも対応できます。

宛先

Platon（オンプレミス版）をご利用のお客様各位

作成

ロゴスウェア株式会社

作成日

2026年11月12日

対象

Platon オンプレミス版

1 本書の目的

2026 年 11 月 11 日、Web サーバーソフトウェア Apache HTTP Server の HTTP/2 通信を処理するモジュール（mod_http2）に、外部から任意のプログラムを実行される可能性のある脆弱性（CVE-2026-119618）が公表されました。

Platon オンプレミス版は Apache HTTP Server 上で動作しており、標準的な手順でインストールした環境では mod_http2 が読み込まれています。速やかに Apache HTTP Server のバージョンアップをお願いいたします。

本書では、何らかの事情で速やかなバージョンアップができない場合の対処として、HTTP/2（mod_http2）を無効化する手順をご案内いたします。

2 要点

要点 1

速やかに Apache HTTP Server のバージョンアップをお願いいたします。これが根本的な対策です。OS に付属する Apache HTTP Server をお使いの場合は、OS の提供元が公開する修正版をご確認のうえ、適用してください。

要点 2

何らかの事情で速やかなバージョンアップができない場合は、3 章の手順で HTTP/2（mod_http2）を無効化することでも対応できます。Platon は HTTP/2 を必要としないため、mod_http2 を無効にしても Platon はそのままご利用いただけます。

要点 3

今回の脆弱性は Apache HTTP Server の HTTP/2 モジュール（mod_http2）の問題で、Platon のプログラムの問題ではありません。

要点 4

弊社がサーバーを運用しているクラウド版（SaaS）は、HTTP/2 の通信が Platon のサーバーまで届かない構成のため、お客様の作業は不要です。

3 バージョンアップができない場合の対処（HTTP/2 の無効化）

何らかの事情で速やかなバージョンアップができない場合は、次の手順で HTTP/2（mod_http2）を無効化してください。以下は AlmaLinux 8 / 9 の標準的な構成の場合の手順です。sudo を実行できる管理者のアカウントで作業してください。無効化の作業は、設定ファイルの名前を 1 つ変更して Apache の設定を再読み込みするだけで、Apache は停止しません。

3.1 現在の状態の確認

```
sudo httpd -M | grep -w http2_module
```

「http2_module (shared)」と表示された場合は、mod_http2 が読み込まれています。3.2 に進んでください。何も表示されない場合は、mod_http2 は読み込まれていないため、作業は不要です。

3.2 無効化

(1) 設定ファイルの名前の変更

mod_http2 を読み込む設定ファイル 10-h2.conf の名前を変更し、読み込まれないようにします。

```
cd /etc/httpd/conf.modules.d
sudo mv 10-h2.conf 10-h2.conf_disabled
```

Apache は、このフォルダの「.conf」で終わるファイルだけを読み込みます。名前の末尾を変えることで、mod_http2 が読み込まれなくなります。

(2) 設定の確認と再読み込み

```
sudo httpd -t && sudo systemctl reload httpd
```

「Syntax OK」と表示され、その後にエラーが表示されなければ、Apache の設定が再読み込みされ、mod_http2 が無効になります。reload のエラー（「Job for httpd.service failed」など）が表示された場合は、無効化は完了していません。3.3 の手順で元に戻し、弊社までお問い合わせください。再読み込みでは Apache は停止しないため、Platon の利用中でも作業できます。

「Syntax OK」以外のエラーが表示された場合は、再読み込みは行われず、Apache はそれまでの設定のまま動き続けます。Apache の設定に H2Direct、H2Push などの「H2」で始まる設定を書いている場合はエラーになりますので、それらの行の先頭に「#」を付けてから、もう一度 (2) を実行してください。原因が分からない場合は、3.3 の手順で元に戻し、弊社までお問い合わせください。

(3) 無効になったことの確認

```
sudo httpd -M | grep -w http2_module
```

(2) の再読み込みがエラーなく終わっていて、このコマンドで何も表示されなければ、mod_http2 は無効になっています。一覧に proxy_http2_module が表示されることがありますが、これは別のモジュールで、残っていて問題ありません。

最後に、ブラウザから Platon にログインし、管理画面・学習画面が問題なく表示されることをご確認ください。

3.3 元に戻す場合

作業後に問題が起きた場合は、ファイルの名前を元に戻して、設定を再読み込みしてください。

```
cd /etc/httpd/conf.modules.d
sudo mv 10-h2.conf_disabled 10-h2.conf
sudo httpd -t && sudo systemctl reload httpd
```

3.4 無効化した後に OS のパッケージを更新する場合のご注意

OS のパッケージを更新（dnf update など）すると、名前を変更した 10-h2.conf が作り直され、mod_http2 が再び読み込まれることがあります。パッケージの更新後は、次のコマンドで確認してください。

```
sudo httpd -M | grep -w http2_module
```

「http2_module (shared)」と表示された場合は、次のコマンドでもう一度無効にしてください。

```
cd /etc/httpd/conf.modules.d
sudo mv -f 10-h2.conf 10-h2.conf_disabled
sudo httpd -t && sudo systemctl reload httpd
```

Platon は HTTP/2 を必要としないため、バージョンアップを行った後も mod_http2 を無効のままご利用いただいて問題ありません。

4 脆弱性の概要

項目	内容
CVE 番号	CVE-2026-119618
対象	Apache HTTP Server の mod_http2（HTTP/2 通信を処理するモジュール）
影響	細工された HTTP/2 通信により、サーバー上で任意のプログラムを実行される可能性
重大度	Critical（Apache Software Foundation の評価）
影響を受けるバージョン（Apache 公式版）	Apache HTTP Server 2.4.55 ～ 2.4.70
修正版（Apache 公式版）	Apache HTTP Server 2.4.71

OS に付属する Apache HTTP Server（dnf でインストールしたもの）は、OS の提供元が独自に修正を取り込むため、バージョン番号が上の表と一致しません。影響の有無と修正版は、お使いの OS の提供元（AlmaLinux、Red Hat など）のセキュリティ情報でご確認ください。

参考情報: https://httpd.apache.org/security/vulnerabilities_24.html

5 お問い合わせ

本書の内容や、HTTP/2 の無効化の手順についてご不明な点がございましたら、弊社の担当営業または Platon サポート窓口までお問い合わせください。

以上