

PHPの脆弱性(CVE-2026-109618、CVE-2026-109619)の QuOLA@Adapter+ への影響について(第二報)

■影響の有無

QuOLA@Adapter+ は、
PHPの脆弱性(CVE-2026-109618、CVE-2026-109619)の影響を受けます。

■影響を受けるバージョン

QuOLA@Adapter+ Ver.6系すべて
セキュリティ情報配信サービス(※1)

※1 対策が完了し、10/24 17時頃から本サービスを再開しました。

■脆弱性の内容

攻撃者が細工したHTTP Requestを QuOLA@Adapter+ に送信することで
製品のサービス停止を引き起こされたり、本製品上で任意のコードを実行されたりするおそれがあります。

■対策

セキュリティ情報配信サービスにつきましては、ご実施いただく応急対策の方法はございません。

QuOLA@Adapter+ を保護するための応急対策として、以下の対応をお願いいたします。

01.
信頼できる範囲外からの、下記画面へのアクセスに対し、WAF等により下記1)～3)の対策を実施する。

- ＜画面＞
- ・セキュリティポリシー管理ツール
 - ・冗長構成管理ツール
 - ・クライアントソフトのダウンロード画面
 - ・NGガイド画面
 - ・その他OS認証(認証情報入力、成功、失敗)画面

- ＜対策＞
- 1)8KB(8,192バイト)を超えるHTTP Request Bodyを含むリクエストをブロックする。
(CVE-2026-109618対策)
- 2)HTTP Request Bodyに「PHP_SESSION_UPLOAD_PROGRESS」が含まれるHTTP POST Requestをブロックする。
(CVE-2026-109619対策)
- 3)HTTP Request BodyまたはCookieのいずれかに「PHPSESSID」が含まれるHTTP POST Requestをブロックする。
(CVE-2026-109619対策)

なお、WAF等の導入方法や設定方法については、QuOLA@Adapter+ の機能ではないため、
技術サポート窓口ではご案内いたしかねますことをご承知おきください。

■恒久対策

問題解決パッチ「v6-bug-fix-5_before.6.06.00.quver」をリリースいたしました。
技術サポートページに公開しておりますので、お客様がご利用中のQuOLA@Adapter+のプライマリサーバーおよびセカンダリサーバーすべてに適用してください。
パッチ適用手順については、同ページに公開しております「QuOLA+_問題解決パッチ(5)インストール手順書.pdf」をご参照ください。

「v6-bug-fix-5_before.6.06.00.quver」は、現在リリース済みのVer.6.00.00～Ver.6.05.01のいずれのバージョンにも適用可能です。
(運用バージョンのバージョンアップを検討されている場合は、バージョンアップ後に「v6-bug-fix-5_before.6.06.00.quver」の適用を推奨します。)