PHPの脆弱性(CVE-2026-109618、CVE-2026-109619)の LOG@Adapter+ / LOG@Adapter+ V7 への影響について(第三報)

■影響の有無
LOG@Adapter+ / LOG@Adapter+ V7 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
LOG@Adapter+ Ver.6系すべて
LOG@Adapter+ V7 Ver.7系すべて

■脆弱性の内容
攻撃者が細工したHTTP Requestを LOG@Adapter+ / LOG@Adapter+ V7 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
応急対策として、以下の対応をご実施ください。

01.
WebUI設定画面において、管理ツールへ接続可能なIPアドレスを、信頼できる範囲のみに制限する。

02.
何らかの理由により信頼できる範囲への制限が困難な場合は、信頼できる範囲外からのアクセスに対し、WAF等により以下の対策を実施する。

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、LOG@Adapter+ / LOG@Adapter+ V7 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
01.
LOG@Adapter+ V7 Ver.7系をご利用中のお客様向け

問題解決パッチ「log-bug-fix-18.lgver」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LOG@Adapter+ V7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「LOG@Adapter+ Ver.7.01 問題解決パッチ(18) パッチインストール手順書.pdf」をご参照ください。

「log-bug-fix-18.lgver」は、LOG@Adapter+ Ver.7.01.00～Ver.7.01.01のいずれかのバージョンに適用可能です。
お客様がご利用中のバージョンがVer.7.00.00の場合は、Ver.7.01.00以降へアップデートした後に本パッチを適用してください。

02.
LOG@Adapter+ Ver.6系をご利用中のお客様向け

問題解決パッチ「log-bug-fix-19.lgver」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LOG@Adapter+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「LOG@Adapter+ Ver.6.10.01 問題解決パッチ(19) インストール手順書.pdf」をご参照ください。

「log-bug-fix-19.lgver」は、LOG@Adapter+ Ver.6.10.01に適用可能です。
お客様がご利用中のバージョンがVer.6.10.00以前の場合は、Ver.6.10.01以降へアップデートした後に本パッチを適用してください。

03.
LOG@Adapter+ Ver.6系 参照専用をご利用中のお客様向け

問題解決パッチ「log-bug-fix-19.lgver」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LOG@Adapter+ 参照専用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「LOG@Adapter+ Ver.6.10.01 問題解決パッチ(19) インストール手順書.pdf」をご参照ください。

「log-bug-fix-19.lgver」は、LOG@Adapter+ 参照専用 Ver.6.10.01に適用可能です。
お客様がご利用中のバージョンがVer.6.10.00以前の場合は、Ver.6.10.01以降へアップデートした後に本パッチを適用してください。