PHPの脆弱性(CVE-2026-109618、CVE-2026-109619)の
RADIUS GUARD S / RADIUS GUARD S V7 への影響について(第二報 修正版)

■影響の有無
RADIUS GUARD S / RADIUS GUARD S 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
RADIUS GUARD S Ver.6系すべて
RADIUS GUARD S V7 Ver.7系すべて

■脆弱性の内容
攻撃者が細工したHTTP Requestを RADIUS GUARD S / RADIUS GUARD S 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、ユーザー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。

※ユーザーツールを使用していない場合でも、管理ツール、ユーザーツール、両方へ接続可能なIPアドレスを、信頼できる範囲のみに制限してください。
WebUI設定画面の詳細については、各バージョンの取扱説明書「3.6.3 WebUI 設定」に記載がございますので、取扱説明書をご参照ください。

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(例:管理ツールは制限できるが、ユーザーツールは制限できない等)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、RADIUS GUARD S / RADIUS GUARD S 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.
RADIUS GUARD S V7 Ver.7系をご利用中のお客様向け

問題解決パッチ「v7-bug-fix-115.acver」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RADIUS GUARD S V7のメインサーバーおよびレプリカ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「RADIUS_GUARD_S_V7_問題解決パッチ(115)インストール手順書.pdf」をご参照ください。

「v7-bug-fix-115.acver」は、現在リリース済みのVer.7.00.00～Ver.7.04.01のいずれのバージョンにも適用可能です。
(「v7-bug-fix-115.acver」を適用するために、最新版へのアップデートは不要です。)

02.
RADIUS GUARD S Ver.6系をご利用中のお客様向け

問題解決パッチ「bug-fix-116.acver」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RADIUS GUARD Sのマスターサーバーおよびスレーブ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「RADIUS GUARD S _問題解決パッチ(116)インストール手順書.pdf」をご参照ください。

「bug-fix-116.acver」は、RADIUS GUARD S Ver.6.18.04専用のパッチです。
お客様がご利用中のバージョンがVer.6.18.03以前の場合は、Ver.6.18.04へアップデートした後に本パッチを適用してください。
(一括アップデートはできないため、各バージョンごとにメンテナンスバージョンを含み1つずつアップデートをしてください。)

【補足説明】
なお、Ver.6.18.04には以下2つの既知の問題が存在します。
Ver.6.18.04にアップデート後、
問題解決パッチ(87)「bug-fix-87.acver」、および、
問題解決パッチ(95)「bug-fix-95.acver」を合わせて適用していただきますよう、お願い申し上げます。
※「bug-fix-87.acver」「bug-fix-95.acver」「bug-fix-116.acver」の適用順はございません。

リリースノート「Account61804-ER001」抜粋
【日付】
2025/05/23

【影響範囲】
Ver.6.18.04
RADIUSプロキシで転送先サーバーを指定し、「障害時状態監視」項目で「Status-Server」または「Request」を設定している場合、
認証時に転送先サーバーから応答がないと、RADIUSサービスが停止する不具合があります。

【回避策】
問題解決パッチ「bug-fix-87.acver」を適用してください。

リリースノート「Account60000-ER430」「Account60000-ER432」抜粋

◇Account60000-ER430

【日付】
2025/07/14

【影響範囲】
Ver.6.00.00以降
ネットワーク設定画面のSSH接続を「許可する」としている場合、
SSH接続に使用するlocaluserのパスワードを知っている管理者または第三者が特定の操作を通じて内部情報を閲覧できる可能性があります。

【回避策】
以下のいずれかで対策してください。
01.問題解決パッチ「bug-fix-91.acver」を適用してください。
02.上記01のパッチを適用できない場合、SSH接続を「許可しない」としてください。
※SSH接続を用いて定期的に自動で情報を取得している場合、上記01で対策して下さい。

◇Account60000-ER432

【日付】
2026/11/28

【影響範囲】
Ver.6.00.00以降
「Account60000-ER430」における対策が不十分だったため、ネットワーク設定画面のSSH接続を「許可する」としている場合、
SSH接続に使用するlocaluserのパスワードを知っている管理者または第三者が特定の操作を通じて内部情報を閲覧できる可能性があります。

【回避策】
以下のいずれかで対策してください。
01.問題解決パッチ「bug-fix-95.acver」を適用してください。
02.上記01のパッチを適用できない場合、SSH接続を「許可しない」としてください。
※SSH接続を用いて定期的に自動で情報を取得している場合、上記01で対策して下さい。
※2025/11/28以前に公開していた、問題解決パッチ「bug-fix-91.acver」では対策が不十分であるため、
「bug-fix-91.acver」ではなく、「bug-fix-95.acver」を適用してください。

なお、「bug-fix-95.acver」は、すでに「bug-fix-91.acver」が適用されている場合でも適用が必要です。

■修正内容
「■恒久対策」の「RADIUS GUARD S Ver.6系をご利用中のお客様向け」の「【補足説明】」において、以下を修正しました。
・既知の問題に対する対策パッチを、問題解決パッチ(91)「bug-fix-91.acver」から問題解決パッチ(95)「bug-fix-95.acver」へ修正しました。
・リリースノート「Account60000-ER432」に関する説明を追記しました。