

2026 年 10 月 26 日

お客様各位

株式会社日立ソリューションズ
Juniper Networks 製品ユーザーサポート

【脆弱性】PHP の脆弱性（CVE-2026-109618／CVE-2026-109619）の影響について(第二報)

平素は Juniper Networks 製品をご利用くださりまして誠にありがとうございます。

PHP の深刻度の高い脆弱性が 2 件（CVE-2026-109618／CVE-2026-109619）公開されています。当該脆弱性に関する Juniper Networks 製品への影響を、以下に案内します。

敬具

記

1. CVE-2026-109618／CVE-2026-109619 の影響

現時点での影響確認状況は以下の通りです。

#	製品	影響を受けるバージョン	対策済バージョン	影響を受ける機能
1	SRX	25.2R1 未満	25.2R1(*1)	J-Web, JSC(*2), fwAuth
2	EX	未発表(*3)	未発表(*3)	J-Web, Captive Portal
3	QFX	未発表(*4)	未発表(*4)	未発表(*4)
4	Mist	調査中(*5)	—	—
5	Junos Space	影響なし	—	—

(*1)25.2 系未満の対策済バージョンは、現時点で発表がありません。

25.2 系以降のバージョンでは、PHP を利用していません。弊社では、25.2 系はリリースしていません。25.4R1 をリリースしています。

(*2)JSC(Juniper Secure Connect)は、リモートアクセス VPN クライアント機能です。

(*3)EX の影響を受けるバージョン/対策済バージョンは現時点で発表がありません。

(*4)QFX は、現時点で発表がありません。

(*5)WAN Assurance について調査中です。

以下の製品は影響を受けないことが確認されています。

- Mist Cloud
- Wireless Assurance
- Wired Assurance
- Access Assurance
- Premium Analytics
- Mist Access Points

2. ワークアラウンド

前述の影響を受ける機能の無効化、または信頼できるホスト及び管理者のみにアクセス制限を行ってください。

3. Juniper Networks 製品セキュリティアドバイザリ

Juniper Networks 製品のセキュリティアドバイザリは、下記 Knowledge Base の Security Advisories(JSA)リンク先のページに掲載されます。

最新の脆弱性情報は以下サイトをご覧ください、適時ご利用環境の対策をいただきますようお願いします。

尚、同サイト記載内容以上の情報は開示されていません。記載内容の解釈また内容等については、弊社サポートではお答えいたしかねます。予めご了承ください。

セキュリティアドバイザリは RSS 配信も行われていますので、併せてご活用ください。

Juniper Networks Support Portal / Knowledge Base

<<https://supportportal.juniper.net/s/knowledge>>

2026-10 Reference Advisory: Status of PHP2Shell vulnerabilities on Juniper Products (CVE-2026-109618, CVE-2026-109619)

<<https://supportportal.juniper.net/s/article/2026-10-Reference-Advisory-Status-of-PHP2Shell-vulnerabilities-on-Juniper-Products-CVE-2026-109618-CVE-2026-109619>>

4. 弊社更新について

弊社においても公開情報を継続して確認し、適宜更新いたします。

以上