

PHP コアのリモートコード実行 (RCE) 脆弱性に対するパッチ (CVE-2026-109618 および
CVE-2026-109619)

Fortinet 社の PSIRT (Product Security Incident Response Team) より Critical として、
以下の情報が公開されましたので、以下の通りご報告させていただきます。

概要：

CVE-2026-109618

PHPでは、メモリ不足 (OOM: Out of Memory) が発生した際に、`longjmp()` を使用して現在の
コンテキストから抜け出し、リクエストの処理を中断します。

一部のコンテキストでは、このような状況が適切に考慮されておらず、メモリ割り当てを実
行する前に、リクエスト用メモリが初期化されていない状態のまま残される可能性があります。
その後のリクエストのクリーンアップ処理において、このメモリが読み取られたり、そ
の内容に基づいて条件分岐が行われたりする可能性があります。

複数のメモリ不足 (OOM) 発生手法によって、この状態を継続的に引き起こすことができ、
結果としてリモートコード実行 (RCE: Remote Code Execution) につながる可能性がありま
す。

深刻度：

CVSS: 9.8 (致命的)

CVE ID：

CVE-2026-109618

影響：

許可されていないコードまたはコマンドを実行する

Fortinetは現在、このCVEがFortinet製品に与える影響について調査を進めています。

調査中の製品 (Products Under Investigation)

- FortiADC
- FortiADC Manager
- FortiClient EMS
- FortiDDoS
- FortiDDoS-F
- FortiSIEM
- FortiMonitor
- FortiClient Cloud
- FortiSOAR
- FortiSOAR PaaS
- FortiGuard
- FortiEndpoint

影響を受けないことが確認されている製品 (Products confirmed NOT Impacted)

- FortiOS
- FortiManager
- FortiAnalyzer
- FortiWeb
- FortiMail
- FortiClient Linux
- FortiClient Windows
- FortiClient MacOS
- FortiSASE
- FortiAuthenticator
- FortiSwitch
- FortiNAC

※本内容は2026年10月22日時点の情報となりますので、今後の最新情報は以下の
メーカー情報をご確認ください。

<https://www.fortiguard.com/psirt/FG-IR-26-186>

以上