



セキュリティ修正

Cisco バグ検索ツールを使用して、未解決の問題、解決済みの問題、およびセキュリティ修正を表示できます。

- Cisco UCS X シリーズ M8、M7、M6 6.0(2.260069)、C シリーズ M8、M7、M6 6.0(2.260069)、および B シリーズ M6 6.0(2.260069) サーバー ファームウェア リリース (2 ページ)
- Cisco UCS B シリーズ M5 サーバー ファームウェア リリース 6.0(1.260012) のセキュリティフィックス (2 ページ)
- Cisco UCS X シリーズ M8、M7、M6 6.0(2.260040)、XE シリーズ M8 6.0(2.260042)、C シリーズ M8、M7、M6 6.0(2.260044)、および B シリーズ M6 6.0(2.260040) サーバー ファームウェア リリースのセキュリティ修正 (3 ページ)
- XE シリーズ M8 サーバファームウェア リリース 6.0(1.260001) のセキュリティ修正：なし (24 ページ)
- C シリーズ M8 サーバファームウェア リリース 6.0(1.250194) のセキュリティ修正：なし (24 ページ)
- Cisco UCS X シリーズ M8、M7 6.0(1.252114)、M6、B シリーズ M66.0(1.250179)、M56.0(1.250169) および C シリーズ M8、M7、M6 6.0(1.250192) サーバファームウェア リリースでセキュリティ修正：なし (24 ページ)
- XE シリーズ M8 6.0(1.251030) サーバファームウェア リリースのセキュリティ修正：なし (24 ページ)
- X シリーズ M8 サーバファームウェア リリース 6.0(1.252039) のセキュリティ修正：なし (24 ページ)
- C シリーズ M8、M7、M6 6.0(1.250174) サーバファームウェア リリースのセキュリティ修正 (24 ページ)
- Cisco UCS X シリーズ M8、M7、M6 6.0(1.250122)、B シリーズ M6、M5 6.0(1.250127) および C シリーズ M8、M7、M6 6.0(1.250131) サーバー ファームウェア リリース：なし (26 ページ)
- Cisco UCS X シリーズ M8、M7、M6 6.0(1.250120)、B シリーズ M6、M5 6.0(1.250126) および C シリーズ M8、M7、M6 6.0(1.250127) サーバー ファームウェア リリース (26 ページ)

Cisco UCS X シリーズ M8、M7、M6 6.0(2.260069)、C シリーズ M8、M7、M6 6.0(2.260069)、および B シリーズ M6 6.0(2.260069) サーバー ファームウェア リリース

欠陥 ID : [CSCwr69876](#)

この製品には、次の Common Vulnerabilities および Exposures (CVE) によって識別される脆弱性の影響を受けるサードパーティ ソフトウェアが含まれています。

CVE ID	説明
CVE-2025-0033	AMD SEV-SNP 内の不適切なアクセス制御により、管理者特権を持つ攻撃者は SNP の初期化中に RMP に書き込みを行うことができ、SEV-SNP ゲストメモリの完全性が失われる可能性があります。
CVE-2025-29943	AMD CPU 内での不適切な書き込み条件の処理により、管理者権限の攻撃者が CPU パイプラインの構成を変更し、SEV-SNP ゲスト内のスタック ポインタを破損する可能性があります。
CVE-2025-48514	SEV ファームウェアでのアクセス制御の粒度が不十分であるため、権限を持つ攻撃者が SNP ゲストを攻撃するための SEV-ES ゲストを作成し、機密性を失う可能性があります。

影響を受けるサードパーティ ソフトウェア コンポーネントを脆弱性の修正が含まれるバージョンにアップグレードする必要があります。製品の今後のバージョンはこの脆弱性の影響を受けません。

Cisco UCS B シリーズ M5 サーバー ファームウェア リリース 6.0(1.260012) のセキュリティ フィックス

Defect ID - [CSCwq34278](#)

この製品には、次の Common Vulnerabilities および Exposures によって識別される脆弱性の影響を受けるサードパーティ ソフトウェアが含まれています：

CVE ID	説明
CVE-2025-20064	特定の Intel リファレンス プラットフォーム上の UEFI FlashUcAcmSmm モジュールでの不適切な入力検証により、権限を持つローカルの攻撃者が任意のコードを実行して権限を昇格させ、システムの機密性、完全性、および可用性に深刻な影響を与える可能性があります。

CVE ID	説明
CVE-2025-20027	特定の Intel リファレンス プラットフォーム上の UEFI WeaERSST モジュールでの不適切な入力検証、特権を持つローカルの攻撃者が権限をエスカレーションし、システムの機密性、完全性、および可用性に影響を与える可能性があります。
CVE-2025-20028	特定の Intel リファレンス プラットフォームの UEFI WhaERST SMM モジュールにおけるチェック時 (TOCTOU) の競合状態により、権限を持つローカルの攻撃者が権限をエスカレーションし、システムの機密性、完全性、および可用性に影響を与える可能性があります。
CVE-2025-20105	Intel リファレンス プラットフォーム上の特定の UEFI ファームウェア SMM モジュールにおける不適切な入力検証により、特権を持つローカルの攻撃者が複雑度の低い任意のコードを実行し、システムの機密性、完全性、および可用性に大きな影響を与える可能性があります。

影響を受けるサードパーティ ソフトウェア コンポーネントを脆弱性の修正が含まれるバージョンにアップグレードする必要があります。製品の今後のバージョンはこの脆弱性の影響を受けません。

Cisco UCS X シリーズ M8、M7、M6 6.0(2.260040)、XE シリーズ M8 6.0(2.260042)、C シリーズ M8、M7、M6 6.0(2.260044)、および B シリーズ M6 6.0(2.260040) サーバー ファームウェア リリースのセキュリティ修正

欠陥 ID : [CSCwr50426](#)

この製品には、次の Common Vulnerabilities および Exposures (CVE) によって識別される脆弱性の影響を受けるサードパーティ ソフトウェアが含まれています。

CVE ID	説明
CVE-2024-13176	OpenSSL の ECDSA 署名の計算におけるタイミングサイドチャネルの脆弱性により、ローカルアクセスまたは低遅延ネットワーク接続を持つ攻撃者が、特に NIST P-521 曲線を使用する場合に、秘密キーを回復する可能性があります。

CVE ID	説明
CVE-2024-5535	OpenSSL の SSL_select_next_proto API 関数のバッファ オーバー読み取りの欠陥により、空のクライアント プロトコル バッファで呼び出される場合にトリガーされ、アプリケーションがクラッシュするか、最大 255 バイトのプライベートメモリがピアに送信される可能性があります。
CVE-2024-9143	OpenSSL で低レベルの GF(2 ^m) 楕円曲線 API を活用、フィールド多項式で信頼されていない明示的な値を使用すると、メモリの読み取りまたは書き込みが境界外に発生し、アプリケーションのクラッシュやリモートコード実行。

影響を受けるサードパーティソフトウェアコンポーネントを脆弱性の修正が含まれるバージョンにアップグレードする必要があります。製品の今後のバージョンはこの脆弱性の影響を受けません。

不具合 ID: CSCwr81218

この製品には、次の Common Vulnerabilities および Exposures (CVE) によって識別される脆弱性の影響を受けるサードパーティソフトウェアが含まれています。

CVE ID	説明
CVE-2025-48384	Git のリンク後ろの脆弱性は、設定ファイルでの改行文字の処理に一貫性がないことに起因します。パスの末尾に改行があるサブモジュールを初期化すると、変更されたパスによって不正なチェックアウト場所が発生し、シンボリックリンクが悪意のあるフックスクリプトを指している場合、任意のコードが実行される可能性があります。

影響を受けるサードパーティソフトウェアコンポーネントを脆弱性の修正が含まれるバージョンにアップグレードする必要があります。製品の今後のバージョンはこの脆弱性の影響を受けません。

欠陥 ID: CSCwr83710

この製品には、次の Common Vulnerabilities および Exposures (CVE) によって識別される脆弱性の影響を受けるサードパーティソフトウェアが含まれています。

CVE ID	説明
CVE-2021-0920	Linuxカーネルの Unix ドメイン ソケット実装 (unix_scm_to_skb inaf_unix.c) の競合状態により、解放済みメモリ使用の脆弱性が発生し、ローカルの攻撃者が権限をエスカレーションしたり、システムクラッシュを引き起こしたりする可能性があります。

CVE ID	説明
CVE-2024-53150	記述子長 (bLength) の不十分な検証に起因する、Linux カーネルの ALSA USB-audio ドライバにおける範囲外読み取りの脆弱性により、物理アクセス権を持つ攻撃者が悪意のある USB デバイスを使用して機密カーネルメモリの破損、またはサービス拒否の原因となります。
CVE-2025-38352	Linux カーネルの POSIX CPU タイマー処理において、handle_posix_cpu_timers() 関数と posix_cpu_timer_del() 関数の間で競合状態（レースコンディション）が発生し、Use-After-Free（解放後使用）の状態を招く可能性があります。これにより、ローカルユーザーが権限を昇格させたり、システムをクラッシュさせたりする恐れがあります。

影響を受けるサードパーティソフトウェアコンポーネントを脆弱性の修正が含まれるバージョンにアップグレードする必要があります。製品の今後のバージョンはこの脆弱性の影響を受けません。

欠陥 ID: CSCws61975

この製品には、次の Common Vulnerabilities および Exposures (CVE) によって識別される脆弱性の影響を受けるサードパーティソフトウェアが含まれています。

CVE ID	説明
CVE-2015-5477	ISC BIND 9 での TKEY クエリの処理エラーにより、リモートの攻撃者がエクスプロイトして REQUIRE アサーションエラーをトリガーし、指定されたデーモンを終了させ、サービス拒否を引き起こす可能性があります。
CVE-2016-2776	ISC BIND 9 が特定のクエリに対する応答を作成する方法の欠陥により、buffer.c でアサーションが失敗する可能性があります。これにより、リモートの攻撃者が指定されたプロセスをクラッシュさせ、予期せず終了する可能性があります。
CVE-2023-50387	「KeyTrap」として知られています。DNSSEC 検証リゾルバ（BIND や Unbound など）に存在するこの脆弱性により、リモート攻撃者が極端な CPU の枯渇とサービス拒否を引き起こす可能性があります。複雑なリソースレコードの組み合わせ。

影響を受けるサードパーティソフトウェアコンポーネントを脆弱性の修正が含まれるバージョンにアップグレードする必要があります。製品の今後のバージョンはこの脆弱性の影響を受けません。

欠陥 ID: CSCws65661

この製品には、次の Common Vulnerabilities および Exposures (CVE) によって識別される脆弱性の影響を受けるサードパーティソフトウェアが含まれています。

CVE ID	説明
CVE-2010-2252	Wget 1.12 以前では、-O（出力先指定）オプションの使用時に、元の URL ではなくリダイレクト先の URL に含まれるファイル名が使用されるため、異なるファイル名を持つ URL への 302 リダイレクトを介して、リモートの攻撃者が任意のファイルに書き込みを行うことが可能です。
CVE-2014-4877	Wget 1.16 より前のバージョンでは、リモート FTP サーバが、再帰的取得中にディレクトリリスト内のシンボリックリンク攻撃を介して任意のファイルに書き込み、コードを実行する可能性があります。
CVE-2016-4971	1.18 より前の Wget では、リモート サーバーは、FTP URL に HTTP 要求をリダイレクトすることで、任意のファイルに書き込むことができます。これにより、Wget は、元の HTTP ファイル名ではなく、FTP サーバーによって指定された名前でファイルを保存します。
CVE-2017-6508	1.19.1 より前の Wget では、リモートの攻撃者が巧妙に細工された URL を介して任意の HTTP ヘッダー（CRLInjection）を挿入でき、セッションハイジャックやその他のヘッダーベースの攻撃につながる可能性があります。
CVE-2018-0494	1.19.5 より前の Wget では、リモートの攻撃者が不正な形式の Set-Cookie ヘッダーを介して意図されている Cookie アクセス制限をバイパス、Cookie のインジェクションまたは上書きを引き起こす可能性があります。
CVE-2021-31879	1.21.1 より前の Wget では、Content-Length などの特定の HTTP 応答ヘッダーが適切に処理されないため、リモートの攻撃者がセキュリティ制御をバイパスたり、予期しない動作を引き起こしたりする可能性があります。
CVE-2024-10524	WPS Office for Windows の特定のバージョンにパストラバーサル脆弱性が存在し、攻撃者が細工されたファイルを介して任意のコードを実行できる。
CVE-2024-38428	1.24.5 より前の Wget には、URI のユーザー情報を適切に解析しないという欠陥に対する脆弱があり、特定の設定でセキュリティフィルタをバイパスたり、ログイン情報の漏洩につながる可能性があります。

影響を受けるサードパーティソフトウェアコンポーネントを脆弱性の修正が含まれるバージョンにアップグレードする必要があります。製品の今後のバージョンはこの脆弱性の影響を受けません。

欠陥 ID : CSCws68419

この製品には、次の Common Vulnerabilities および Exposures（CVE）によって識別される脆弱性の影響を受けるサードパーティソフトウェアが含まれています。

CVE ID	説明
CVE-2009-5155	GNU C ライブラリ (glibc) の <code>strfmon_l</code> 関数の off-by-1 エラーにより、コンテキスト依存の攻撃者は、サービス拒否 (クラッシュ) を引き起こしたり、大きな精度の値を介して任意のコードを実行したりする可能性があります。
CVE-2010-0015	GNU C ライブラリ (glibc) での NIS+ の実装により、リモートの攻撃者は、バッファオーバーフローをトリガーする巧妙に細工された NIS+ディレクトリ名を介して、サービス拒否 (クラッシュ) を引き起こしたり、任意のコードを実行したりすることが可能です。
CVE-2011-5320	1.20.0 より前のBusyBoxの <code>tar</code> の実装では、リモートの攻撃者が <code>tar</code> ヘッダーへのディレクトリトラバーサル攻撃を介して任意のファイルを作成または上書きようになります。
CVE-2012-4412	GNU C ライブラリ (glibc) の <code>strcoll</code> 関数での整数オーバーフローにより、コンテキスト依存の攻撃者は、サービス拒否 (クラッシュ) を引き起こしたり、長い文字列を介して任意のコードを実行したりする可能性があります。
CVE-2012-4424	GNU C ライブラリ (glibc) の <code>strcoll</code> 関数でのスタックベースのバッファオーバーフローにより、コンテキスト依存の攻撃者は、サービス拒否 (クラッシュ) を引き起こしたり、長い文字列を介して任意のコードを実行したりする可能性があります。
CVE-2013-4237	GNU C ライブラリ (glibc) の <code>read_dir_r</code> 関数は、特定のディレクトリエントリを適切に処理しません。そのため、コンテキスト依存の攻撃者が、サービス拒否 (境界外の読み取りとクラッシュ) を引き起こす可能性があります。
CVE-2013-4458	GNU C ライブラリ (glibc) の <code>getaddrinfo</code> 関数のスタックベースのバッファオーバーフローにより、リモートの攻撃者は多数の AF_INET6 アドレスを介してサービス拒否 (クラッシュ) を引き起こすことができます。
CVE-2013-4788	GNU C ライブラリ (glibc) の PTR-MANGLE 実装は、ガード値を適切に初期化しないため、ローカルの攻撃者は、ポインタガード保護メカニズムをバイパスできます。
CVE-2014-4043	2.20 より前の GNU C ライブラリ (glibc) の <code>posix_spwn_file_actions_addopen</code> 関数は、その <code>path</code> 引数をコピーしないため、コンテキスト依存の攻撃者は、解放済みメモリ使用後の脆弱性をトリガーできます。

CVE ID	説明
CVE-2014-6040	GNU C ライブラリ (glibc) の iconv 関数における範囲外の読み取りにより、コンテキスト依存の攻撃者は、巧妙に細工されたマルチバイトシーケンスを介してサービス拒否（クラッシュ）を引き起こすことができます。
CVE-2014-7817	GNU C ライブラリ (glibc) の wordexp 関数により、コンテキスト依存の攻撃者は、WRDE_NOCMD が指定されている場合でも、コマンド置換をトリガーする巧妙に細工された文字列を介して任意のコマンドを実行できます。
CVE-2014-8121	GNU C ライブラリ (glibc) の nss_files 実装は、特定のデータベースファイルを適切に処理しません。そのため、ローカルの攻撃者は、サービス拒否（無限ループ）を引き起こしたり、データベースを破損したりする可能性があります。
CVE-2014-9402	GNU C ライブラリ (glibc) の getnetbyname 関数を使用すると、リモートの攻撃者は、巧妙に細工された DNS 応答を介して、サービス拒否（無限ループ）を引き起こすことができます。
CVE-2014-9761	GNU C ライブラリ (glibc) の Ann 関数におけるスタックベースのバッファオーバーフローにより、コンテキスト依存の攻撃者は、長い文字列を介してサービス拒否（クラッシュ）を引き起こすことができます。
CVE-2015-1781	GNU C ライブラリ (glibc) の gethostbyname_r 関数でのバッファオーバーフローにより、コンテキスト依存の攻撃者は、サービス拒否（クラッシュ）を引き起こしたり、長いホスト名を介して任意のコードを実行したりする可能性があります。
CVE-2015-5180	GNU C ライブラリ (glibc) の resquery 関数での NULL ポインタ逆参照により、リモートの攻撃者は、巧妙に細工された DNS 応答を介して、サービス拒否（クラッシュ）を引き起こすことができます。
CVE-2015-8776	GNU C ライブラリ (glibc) の strftime 関数での範囲外アクセスにより、コンテキスト依存の攻撃者は、巧妙に細工されたフォーマット文字列を介して、サービス拒否（クラッシュ）を引き起こすことができます。
CVE-2015-8777	GNU C ライブラリ (glibc) の LD_PointER_GUARD 環境変数、ローカルの攻撃者は、ポインタガード保護メカニズムを無効にしてバイパスすることができます。
CVE-2015-8778	GNU C ライブラリ (glibc) の hcreate 関数での整数オーバーフローにより、コンテキスト依存の攻撃者は、多数の要素を介して、サービス拒否（クラッシュ）を引き起こしたり、任意のコードを実行したりする可能性があります。

CVE ID	説明
CVE-2015-8779	GNU C ライブラリ (glibc) の <code>catopen</code> 関数でのスタックベースのバッファオーバーフローにより、コンテキスト依存の攻撃者は、サービス拒否 (クラッシュ) を引き起こしたり、長いカタログ名を介して任意のコードを実行したりする可能性があります。
CVE-2015-8982	GNU C ライブラリ (glibc) の <code>strftime</code> 関数でバッファオーバーフローにより、コンテキスト依存の攻撃者は、巧妙に細工されたフォーマット文字列を介して、サービス拒否 (クラッシュ) を引き起こすことができます。
CVE-2015-8983	GNU C ライブラリ (glibc) の <code>_IO_wstr_overflow</code> 関数での整数オーバーフローにより、コンテキスト依存の攻撃者は、大きな文字列を介して、サービス拒否 (クラッシュ) を生じさせることや、おそらくは任意のコードを実行することが可能になります。
CVE-2015-8984	GNU C ライブラリ (glibc) の <code>fnmatch</code> 関数における範囲外の読み取りにより、コンテキスト依存の攻撃者は、巧妙に細工されたパターンを介して、サービス拒否 (クラッシュ) を引き起こすことができます。
CVE-2015-8985	GNU C ライブラリ (glibc) の <code>pop_fail_stack</code> 関数により、コンテキスト依存の攻撃者は、拡張正規表現処理に関連するベクトルを介してサービス拒否 (アサーションの失敗とクラッシュ) を引き起こすことができます。
CVE-2016-10228	GNU C ライブラリ (glibc) の <code>iconv</code> 関数における範囲外への書き込みにより、コンテキスト依存の攻撃者は、サービス拒否 (クラッシュ) を引き起こしたり、細工されたマルチバイトシーケンスを介して任意のコードを実行したりする可能性があります。
CVE-2016-10739	GNU C ライブラリ (glibc) の <code>getaddrinfo</code> 関数のバッファオーバーフローにより、リモートの攻撃者は多数の <code>AF_INET6</code> アドレスを介してサービス拒否 (クラッシュ) を引き起こすことができます。
CVE-2016-1234	GNU C ライブラリ (glibc) の <code>glob</code> 関数でのスタックベースのバッファオーバーフローにより、コンテキスト依存の攻撃者は、サービス拒否 (クラッシュ) を引き起こしたり、長いパスを介して任意のコードを実行したりする可能性があります。
CVE-2016-3075	GNU C ライブラリ (glibc) の <code>getnetbyname</code> 関数におけるスタックベースのバッファオーバーフローにより、リモートの攻撃者は、巧妙に細工された DNS 応答を介して、サービス拒否 (クラッシュ) を引き起こすことができます。

CVE ID	説明
CVE-2016-3706	GNU C Library (glibc) の <code>getaddrinfo</code> 関数において、CVE-2013-4458 に対する修正が不完全であったことに起因するスタックベースのバッファオーバーフローが存在します。これにより、リモートの攻撃者は <code>hostent</code> 変換を伴う攻撃経路を通じて、サービス拒否（クラッシュ）を引き起こす可能性があります。
CVE-2016-4429	GNU C ライブラリ (glibc) の <code>clntudp_call</code> 関数でのスタックベースのバッファオーバーフローにより、リモートの攻撃者は、巧妙に細工された RPC 応答を介して、サービス拒否（クラッシュ）を引き起こすことができます。
CVE-2017-12132	2.26 より前の GNU C ライブラリ (glibc) の DNS スタブリゾルバは、EDNS サポートが有効になっている場合に大きな UDP 応答を要求し、IP フラグメンテーションによるオフパス DNS スプーフィング攻撃を簡素化する可能性があります。
CVE-2017-15670	2.27 より前の GNU C ライブラリ (glibc) の <code>glob</code> 関数の <code>off-by-1</code> エラーにより、~ 演算子とその後の長い文字列を使用してホームディレクトリを処理する際にヒープベースのバッファオーバーフローが発生する。
CVE-2017-15671	2.27 より前の GNU C ライブラリ (glibc) の <code>glob</code> 関数は、長いユーザー名を持つ ~ 演算子を処理するときに、割り当てられたメモリの解放をスキップし、サービス拒否（メモリリーク）につながる可能性があります。
CVE-2017-16997	GNU C ライブラリ (glibc) の <code>elf/dl-load.c</code> 実装は、特定のチェックを適切に処理しないため、ローカルの攻撃者は、巧妙に細工された共有オブジェクトを介してセキュリティ制限をバイパスできます。
CVE-2017-8804	x86_64 の GNU C ライブラリ (glibc) の <code>memmove</code> と <code>memcpy</code> の実装では、場合によっては重複するメモリ領域が適切に処理されません。そのため、コンテキスト依存の攻撃者が、サービス拒否（クラッシュ）を引き起こす可能性があります。また、特定できないその他の影響を及ぼす可能性もあります。
CVE-2018-1000001	GNU C ライブラリ (glibc) の <code>realpath</code> 関数でのバッファアンダーフローにより、ローカルの攻撃者が、サービス拒否（クラッシュ）を引き起こしたり、巧妙に細工されたパスを介して任意のコードを実行したりする可能性があります。
CVE-2018-11236	GNU C ライブラリ (glibc) の <code>"vfprintf_internal"</code> 関数での整数オーバーフローにより、コンテキスト依存の攻撃者は、サービス拒否（クラッシュ）を引き起こしたり、大きな精度の値を介して任意のコードを実行したりする可能性があります。

CVE ID	説明
CVE-2018-6485	GNU C ライブラリ (glibc) 2.26 以前の <code>posix_memalign</code> 関数の実装での整数オーバーフローにより、これらの関数が小さすぎるヒープ領域へのポインタを返す可能性があり、ヒープの破損につながる可能性があります。
CVE-2019-1010023	GNU C ライブラリ (glibc) の <code>ld.so</code> ダイナミックローダーでのバッファオーバーフローにより、ローカルの攻撃者は、サービス拒否 (クラッシュ) を引き起こしたり、巧妙に細工された環境変数を介して任意のコードを実行したりする可能性があります。
CVE-2019-19126	2.31 より前の GNU C ライブラリ (glibc) は、SUID バイナリの <code>LD_PRELOAD</code> 環境変数を適切に処理しないため、ローカルの攻撃者はセキュリティ制限をバイパスできます。
CVE-2019-25013	EUC-KR 文字セットに変換する際の GNU C ライブラリ (glibc) の <code>iconv</code> 関数でのバッファオーバーフローにより、コンテキスト依存の攻撃者が、サービス拒否 (クラッシュ) を引き起こしたり、任意のコードを実行したりする可能性があります。
CVE-2019-9169	GNU C ライブラリ (glibc) の <code>regcomp</code> 関数により、コンテキスト依存の攻撃者は、巧妙に細工された正規表現を介して、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。
CVE-2020-10029	GNU C ライブラリ (glibc) の <code>cosl</code> 関数でのスタックベースのバッファオーバーフローにより、コンテキスト依存の攻撃者が、大きな入力値を介して、サービス拒否 (クラッシュ) を引き起こしたり、任意のコードを実行したりする可能性があります。
CVE-2020-1751	GNU C ライブラリ (glibc) の <code>dl_open</code> 関数でのスタックベースのバッファオーバーフローにより、ローカルの攻撃者が、サービス拒否 (クラッシュ) を引き起こしたり、細工された共有オブジェクトパスを介して任意のコードを実行したりする可能性があります。
CVE-2020-1752	GNU C ライブラリ (glibc) の <code>glob</code> 関数の解放済み脆弱性により、コンテキスト依存の攻撃者は、サービス拒否 (クラッシュ) を引き起こしたり、巧妙に細工されたパスを介して任意のコードを実行したりする可能性があります。
CVE-2020-27618	IBM1364 文字セットに変換する際の GNU C ライブラリ (glibc) の <code>iconv</code> 関数でのバッファオーバーフローにより、コンテキスト依存の攻撃者が、サービス拒否 (クラッシュ) を引き起こしたり、任意のコードを実行したりする可能性があります。

CVE ID	説明
CVE-2020-29573	GNU C ライブラリ (glibc) の printf 関数でバッファ オーバーフローが発生し、コンテキスト依存の攻撃者が大きな精度の値を介してサービス拒否 (クラッシュ) を引き起こす可能性があります。
CVE-2021-27645	GNU C ライブラリ (glibc) の nscd (ネーム サービス キャッシュデーモン) におけるダブルフリーの脆弱性により、ローカルの攻撃者が、サービス拒否 (クラッシュ) を引き起こしたり、任意のコードを実行したりする可能性があります。
CVE-2021-3326	ISO-2022-JP-3 文字セットに変換する際の GNU C ライブラリ (glibc) の iconv 関数でのバッファ オーバーフローにより、コンテキスト依存の攻撃者が、サービス拒否 (クラッシュ) を引き起こしたり、任意のコードを実行したりする可能性があります。
CVE-2021-33574	GNU C ライブラリ (glibc) の mq_notify 関数における解放済みの脆弱性により、コンテキスト依存の攻撃者が、サービス拒否 (クラッシュ) を引き起こしたり、任意のコードを実行したりする可能性があります。
CVE-2021-35942	GNU C ライブラリ (glibc) の wordexp 関数でバッファ オーバーフローにより、コンテキスト依存の攻撃者が長い文字列を介してサービス拒否 (クラッシュ) を引き起こす可能性があります。
CVE-2021-3999	GNU C ライブラリ (glibc) の getcwd 関数でのバッファ オーバーフローにより、ローカルの攻撃者は、サービス拒否 (クラッシュ) を引き起こしたり、長いパスを介して任意のコードを実行したりする可能性があります。
CVE-2022-23218	GNU C ライブラリ (glibc) の svcunix_create 関数におけるスタックベースのバッファ オーバーフローにより、リモートの攻撃者は、巧妙に細工された RPC 要求を介して、サービス拒否 (クラッシュ) を引き起こすことができます。
CVE-2022-23219	GNU C ライブラリ (glibc) の clnt_create 関数でのスタックベースのバッファ オーバーフローにより、リモートの攻撃者は、巧妙に細工された RPC 要求を介して、サービス拒否 (クラッシュ) を引き起こすことができます。
CVE-2023-4527	GNU C ライブラリ (glibc) の getaddrinfo 関数のスタックベースのバッファ オーバーフローにより、リモートの攻撃者は、TCP を介して受信した大きな DNS 応答を介して、サービス拒否 (クラッシュ) を引き起こすことができます。
CVE-2023-4806	GNU C ライブラリ (glibc) の getaddrinfo 関数の解放済み脆弱性により、リモートの攻撃者は、巧妙に細工された DNS 応答を介してサービス拒否 (クラッシュ) を引き起こすことができます。

CVE ID	説明
CVE-2023-4813	GNU C ライブラリ (glibc) の <code>getaddrinfo</code> 関数の解放済み脆弱性により、リモートの攻撃者は、巧妙に細工された DNS 応答を介してサービス拒否（クラッシュ）を引き起こすことができます。
CVE-2023-4911	GLIBC_TUNABLES環境変数の処理中に GNU C ライブラリのダイナミックローダー <code>ld.so</code> でバッファ オーバーフローが発生し、ローカルの攻撃者が昇格された権限で任意のコードを実行できるようになります。
CVE-2023-5156	GNU C ライブラリ (glibc) の <code>getaddrinfo</code> 関数のメモリリークにより、リモートの攻撃者は、巧妙に細工された DNS 応答を介して、サービス拒否（メモリの枯渇）を引き起こすことができます。
CVE-2024-2961	ISO-2022-CN-EXT 文字セットに変換する際の GNU C ライブラリ (glibc) の <code>iconv</code> 関数でのバッファ オーバーフローにより、コンテキスト依存の攻撃者が、サービス拒否（クラッシュ）を引き起こしたり、任意のコードを実行したりする可能性があります。
CVE-2024-33599	GNU C ライブラリ (glibc) の <code>nscd</code> （ネーム サービス キャッシュ デーモン）におけるバッファ オーバーフローにより、ローカルの攻撃者が、サービス拒否（クラッシュ）を生じさせることや、おそらくは任意のコードを実行することが可能になります。
CVE-2024-33600	GNU C ライブラリ (glibc) の <code>nscd</code> （ネーム サービス キャッシュ デーモン）における NULL ポインタの逆参照により、ローカルの攻撃者は、巧妙に細工された要求を介して、サービス拒否（クラッシュ）を引き起こすことができます。
CVE-2024-33601	GNU C ライブラリ (glibc) の <code>nscd</code> （ネーム サービス キャッシュ デーモン）におけるバッファ オーバーフローにより、ローカルの攻撃者が、サービス拒否（クラッシュ）を生じさせることや、おそらくは任意のコードを実行することが可能になります。
CVE-2024-33602	GNU C ライブラリ (glibc) の <code>nscd</code> （ネーム サービス キャッシュ デーモン）におけるバッファ オーバーフローにより、ローカルの攻撃者が、サービス拒否（クラッシュ）を生じさせることや、おそらくは任意のコードを実行することが可能になります。
CVE-2025-0395	GNU C ライブラリ (glibc) バージョン 2.13 から 2.40 の <code>assert ()</code> 関数でバッファ オーバーフローが発生します。これは、失敗メッセージに十分なスペースが割り当てられていないためで、サービス拒否につながる可能性があります。

CVE ID	説明
CVE-2025-4802	GNU C ライブラリ (glibc) バージョン 2.27~2.38 の脆弱性により、ローカルの攻撃者は、悪意のある共有ライブラリをロードし、静的にコンパイルされた <code>setuid</code> バイナリ内の <code>dlopen</code> を呼び出す信頼できない <code>LD_LIBRARY_PATH</code> を介して権限を昇格させることができます。
CVE-2025-5702	GNU C ライブラリ (glibc) バージョン 2.39 以降の Power10 プロセッサ用に最適化された <code>strcmp</code> 実装における脆弱性により、ベクトルレジスタが不適切に初期化され、データの破損や制御フローの変更が発生する可能性があります。
CVE-2025-8058	GNU C ライブラリ (glibc) バージョン 2.4~2.41 の <code>regcomp</code> 関数でのダブルフリーの脆弱性は、メモリ割り当て障害が発生した場合にブラケットの解析中に発生し、任意のコードが実行される可能性があります。

影響を受けるサードパーティ ソフトウェア コンポーネントを脆弱性の修正が含まれるバージョンにアップグレードする必要があります。製品の今後のバージョンはこの脆弱性の影響を受けません。

欠陥 ID : [CSCws68836](#)

この製品には、次の Common Vulnerabilities および Exposures (CVE) によって識別される脆弱性の影響を受けるサードパーティ ソフトウェアが含まれています。

CVE ID	説明
CVE-2007-5116	Perl 5.8 の正規表現エンジン (<code>regcomp.c</code>) のポリモーフィック型イック オプコードのサポートにおけるバッファ オーバーフローにより、コンテキスト依存の攻撃者は、正規表現のバイトを Unicode (UTF) 文字に切り替えることで任意のコードを実行することが可能になります。
CVE-2008-1927	Perl 5.8.8 の Double Free 脆弱性により、コンテキスト依存の攻撃者は、UTF-8 文字を含む巧妙に細工された正規表現を使用して、サービス拒否 (メモリ破損とクラッシュ) を引き起こすことができます。
CVE-2008-5302	Perl 5.8.8 および 5.10.0 の <code>File::Path</code> の <code>rmtree</code> 関数の競合状態により、ローカル ユーザーがシンボリックリンク攻撃を介して任意の <code>setuid</code> バイナリを作成できる。
CVE-2008-5303	Perl 5.8.8 の <code>File::Path</code> の <code>rmtree</code> 関数の競合状態により、ローカル ユーザーは、以前のセキュリティ修正の回帰を表すシンボリックリンク攻撃を介して任意のファイルを削除できるようになります。

CVE ID	説明
CVE-2010-1168	Perl 向けの 2.25 以前の Safe (別名 Safe.pm) モジュールにより、コンテキスト依存の攻撃者は、意図されたアクセス制限をバイパス、DESTROY や AUTOLOAD などの暗黙的なメソッドを含むベクトルを介して任意のコードを実行できます。
CVE-2010-1447	Perl 用の Safe (別名 Safe.pm) モジュール 2.26 以前により、コンテキスト依存の攻撃者はアクセス制限をバイパスし、サブルート参照や遅延実行を含むベクトルを介して任意のコードを実行できます。
CVE-2010-2761	3.50 より前の CGI.pm の multipart_init 関数は、ハードコードされた MIME 境界文字列を使用します。これにより、リモートの攻撃者は任意の HTTP ヘッダーを挿入し、HTTP 応答分割攻撃を実行できます。
CVE-2010-4410	3.50 より前の CGI.pm のヘッダー機能における CRLF インジェクションの脆弱性により、リモートの攻撃者は任意の HTTP ヘッダーを挿入し、改行文字を介して HTTP 応答分割攻撃を実行できます。
CVE-2011-0761	Perl 5.10.x では、コンテキスト依存の攻撃者が、getpeername、readdir、Closedir などの関数に引数を挿入することにより、サービス拒否 (NULL ポインタの逆参照とクラッシュ) を引き起こすことができます。
CVE-2011-1487	Perl 5.10.x ~ 5.13.x の lc、lcfirst、uc、および ucfirst 関数は、リターン値に taint 属性を適用しないため、攻撃者は巧妙に細工された文字列を使用して汚染保護メカニズムをバイパスできます。
CVE-2011-2939	Perl の Encode モジュールの decode_xs 関数の off-by-one エラーにより、コンテキスト依存の攻撃者は、巧妙に細工された Unicode 文字列を介してサービス拒否 (メモリ破損) を引き起こしたり、任意のコードを実行したりできます。
CVE-2011-3597	Perl の 1.17 より前の Digest モジュールにおける eval インジェクションの脆弱性により、コンテキスト依存の攻撃者が新しいコンストラクタを介して任意のコマンドを実行できる。
CVE-2011-4116	Perl の File::Temp モジュールの _is_safe 関数がシンボリック リnk を適切に処理しないため、ローカルの攻撃者がセキュリティチェックをバイパス可能性があります。
CVE-2012-5195	Perl の Perl.Repeatcpy 関数でのヒープベースのバッファ オーバーフローにより、コンテキスト依存の攻撃者が、「x」文字列のリピート演算子を介してサービス拒否を引き起こしたり、任意のコードを実行したりできるようになります。

CVE ID	説明
CVE-2012-5526	Perl 用の 3.63 より前の CGI.pm は、Set-Cookie または P3P ヘッダーの改行を適切にエスケープしないため、リモートの攻撃者が任意のヘッダーを HTTP 応答に挿入できます。
CVE-2012-6329	Perl 5.17.7 より前の Locale::Maketext の実装では、バックスラッシュとメソッド名が適切に処理されないため、コンテキスト依存の攻撃者は、巧妙に細工された変換文字列を介して任意のコマンドを実行できます。
CVE-2013-1667	Perl 5.8.2 ~ 5.16.x の再ハッシュメカニズムにより、コンテキスト依存の攻撃者は、巧妙に細工されたハッシュキーを介してサービス拒否（メモリ消費とクラッシュ）を引き起こすことができます。
CVE-2013-7422	Perl 5.20 より前の正規表現エンジン（regcomp.c）の整数アンダーフローにより、コンテキスト依存の攻撃者が任意のコードを実行したり、長い桁列を介してサービス拒否を引き起こしたりできるようになります。
CVE-2014-4330	2.154 より前の Data::Dumper の Dumper メソッドにより、コンテキスト依存の攻撃者が、深くネストされた Array-Reference を介してサービス拒否（スタックの枯渇とクラッシュ）を引き起こす可能性があります。
CVE-2015-8853	Perl 5.24.0 より前の正規表現エンジンでは、コンテキスト依存の攻撃者が、巧妙に細工された UTF-8 データを介してサービス拒否（無限ループと高い CPU 使用率）を引き起こすことができます。
CVE-2016-1238	Perl 5.x（5.22.3 より前および 5.24.1）は、モジュール包含パス（@INC）からカレントディレクトリ（「.」）を適切に削除しないため、ローカルユーザは、トロイの木馬モジュールを介して権限を取得できます。
CVE-2016-2381	Perl は、コンテキスト依存の攻撃者が、envp 配列の重複した環境変数を使用し、子プロセスの汚染保護メカニズムをバイパスさせる可能性があります。
CVE-2016-6185	Perl の XSLoader::load メソッドは、文字列 eval で呼び出されたときに共有オブジェクト（.so）ファイルを適切に検索しないため、ローカルユーザが悪意のあるライブラリを介して任意のコードを実行できる可能性があります。
CVE-2018-12015	Perl 5.26.2 までの Archive::Tar モジュールのため、リモートの攻撃者はディレクトリ トラバーサル保護をバイパスし、シンボリック リンクと同じ名前の通常のファイルを含むアーカイブを介して任意のファイルを上書きできます。

CVE ID	説明
CVE-2018-18311	Perl 5.26.3 および 5.28.1 より前には、無効な書き込み操作をトリガーする巧妙に細工された正規表現を介したバッファ オーバーフローの脆弱性があります。
CVE-2018-6913	Perl 5.26.2 より前の <code>pack</code> 関数のヒープベースのバッファ オーバーフローにより、コンテキスト依存の攻撃者は、大きな項目数を介して任意のコードを実行できるようになります。
CVE-2020-10543	Perl 5.30.3 より前の 32 ビット プラットフォームでは、ネストされた正規表現修飾子に整数オーバーフローがあるため、ヒープベースのバッファ オーバーフローが発生します。
CVE-2020-10878	5.30.3 より前の Perl には、正規表現エンジンでの特定の命令の誤った処理に関連する整数オーバーフローがあり、命令インジェクションにつながる可能性があります。
CVE-2020-12723	Perl 5.30.3 より前の正規表現コンパイラ (<code>regcomp.c</code>) では、 <code>S_study_chunk</code> の再帰的呼び出し中に、バッファ オーバーフローの脆弱性が発生します。
CVE-2020-16156	CPAN 2.28 では、署名検証のバイパスが可能です。これにより、攻撃者は、ネットワークからダウンロードした Perl モジュールのセキュリティチェックをバイパスできる可能性があります。
CVE-2023-31484	CPAN.pm (2.35 より前) および Perl (5.38.0 より前) は、HTTPS を介してディストリビューションをダウンロードするときに TLS 証明書を検証しないため、ユーザが中間者攻撃にさらされます。
CVE-2023-47038	不正な Unicode プロパティを使用して巧妙に細工された正規表現をコンパイルする場合に、Perl 5.30.0 ~ 5.38.0 でヒープベースのバッファ オーバーフローの脆弱性が見つかりました。
CVE-2024-56406	Perl の <code>tr</code> 演算子におけるヒープ バッファ オーバーフローの脆弱性は、非 ASCII バイトを処理する際に発生し、サービス拒否や任意のコード実行につながる可能性があります。
CVE-2025-40909	Perl スレッドにおけるディレクトリ ハンドル複製時の競合状態により、現在の作業ディレクトリが予期せず変更される可能性があります。これにより、ローカル攻撃者がスレッドに悪意のあるコードを読み込ませるよう仕向ける恐れがあります。影響を受けるサードパーティ製ソフトウェアコンポーネントは、この脆弱性への修正を含むバージョンに更新されました。製品の今後のバージョンはこの脆弱性の影響を受けません。

欠陥 ID : [CSCwr84274](#)

この製品には、次の Common Vulnerabilities および Exposures (CVE) によって識別される脆弱性の影響を受けるサードパーティ ソフトウェアが含まれています。

CVE ID	説明
CVE-2025-27363	FreeType バージョン 2.13.0 以下の範囲外書き込みの脆弱性は、TrueType GX および可変フォントファイルのフォント subglyph 構造を解析するときに発生します。不適切なデータ型の割り当ては、バッファのラップアラウンドとヒープ割り当ての上限につながり、任意のコード実行を許可する可能性があります。

影響を受けるサードパーティ ソフトウェア コンポーネントを脆弱性の修正が含まれるバージョンにアップグレードする必要があります。製品の今後のバージョンはこの脆弱性の影響を受けません。

欠陥 ID : [CSCwr84317](#)

この製品には、次の Common Vulnerabilities および Exposures (CVE) によって識別される脆弱性の影響を受けるサードパーティ ソフトウェアが含まれています。

CVE ID	説明
CVE-2023-38545	curl の SOCKS5 プロキシハンドシェイクにおけるシビラティ（重大度）の高いヒープベースのバッファ オーバーフローの脆弱性は、低速なハンドシェイク時に 255 バイトを超えるホスト名がターゲット バッファに誤ってコピーされると発生し、悪意のあるプロキシがクライアントで任意のコードを実行する可能性があります。

影響を受けるサードパーティ ソフトウェア コンポーネントを脆弱性の修正が含まれるバージョンにアップグレードする必要があります。製品の今後のバージョンはこの脆弱性の影響を受けません。

Defect ID - [CSCwq11344](#)

この製品には、次の Common Vulnerabilities および Exposures (CVE) によって識別される脆弱性の影響を受けるサードパーティ ソフトウェアが含まれています。

CVE ID	説明
CVE-1999-0289	Win32 用の Apache Web サーバは、要求された URL にドット (.) が付加されている場合、制限されたファイルへのアクセスを提供する可能性があり、不正なファイル開示を許可する可能性があります。
CVE-1999-0678	Debian GNU/ Linux 上の Apache のデフォルト設定では、ServerRoot が to/usr/doc に設定されます。これにより、リモートユーザーはサーバ全体のドキュメント ファイルを読み取ることができます。

CVE ID	説明
CVE-2010-1151	Apache HTTP サーバの <code>mod_auth_shadow</code> モジュールの競合状態により、リモートの攻撃者は認証をバイパス、外部ヘルパーアプリケーションとの不適切な対話によってデータを読み取りまたは変更することができます。
CVE-2023-31122	Apache HTTP サーババージョン 2.4.57 までの <code>mod_macro</code> モジュールにおける範囲外の読み取りの脆弱性により、攻撃者が長いマクロの処理時にクラッシュを引き起こしたり、機密情報を取得したりする可能性があります。
CVE-2023-38709	バージョン 2.4.58 までの Apache HTTP サーバのコアにおける入力検証の失敗により、悪意のある、またはエクスプロイト可能なバックエンドコンテンツ ジェネレータが HTTP 応答を分割し、キャッシュポイズニングや XSS につながる可能性があります。
CVE-2023-43622	<code>mod_http2</code> モジュールの欠陥により、攻撃者は初期ウィンドウ サイズが 0 で HTTP/2 接続を開き、その接続の処理を無期限にブロックし、「slow loris」形式の攻撃でワーカー リソースを使い果たします。
CVE-2023-45802	クライアントによって HTTP/2 ストリームがリセットされても、メモリ リソースがすぐに再要求されないことがあります。これにより、クライアントは、サーバのメモリフットプリントを増加させ、サービス拒否を引き起こす可能性があります。
CVE-2024-24795	複数の Apache HTTP サーバモジュールに存在する HTTP 応答分割の脆弱性により、攻撃者は悪意のある応答ヘッダーをバックエンドアプリケーションに挿入し、結果として HTTP 非同期攻撃を引き起こします。
CVE-2024-27316	Apache HTTP サーバは、単一ストリーム内で送信される HTTP/2 CONTINUATION フレームの量を制限できません。これにより、メモリが枯渇し、サービス妨害状態が発生する可能性があります。
CVE-2024-36387	Apache HTTP サーバで HTTP/2 接続を介して WebSocket プロトコルのアップグレードを提供すると、Null ポインタの逆参照が発生し、サーバ プロセスがクラッシュする可能性があります。
CVE-2024-38472	Windows の Apache HTTP Server における Server-Side Request Forgery (SSRF) の脆弱性により、攻撃者は巧妙に細工されたリクエストまたはコンテンツを介して悪意のあるサーバに NTLM ハッシュをリークする可能性があります。

CVE ID	説明
CVE-2024-38473	mod_proxy モジュールでのエンコーディングの問題により、エンコーディングが正しくない要求 URL がバックエンドサービスに送信され、巧妙に細工された要求を介して認証をバイパスする可能性があります。
CVE-2024-38474	mod_rewrite における置換エンコーディングの問題により、攻撃者は、設定によって許可されているが、URL によって直接到達できないディレクトリでスクリプトを実行したり、CGI の実行のみを目的としたスクリプト ソース コードを開示したりできます
CVE-2024-38475	mod_rewrite での出力のエスケープが不適切なため、攻撃者は、提供は許可されているが直接到達することを意図していないファイルシステムの場所に URL をマッピングし、コードが実行される可能性があります。
CVE-2024-38476	Apache HTTP サーバーのコアにおける脆弱性により、悪意のある応答ヘッダーまたはエクスプロイト可能なバックエンドアプリケーションを介した情報漏洩、SSRF、またはローカル スクリプトの実行が可能になります。
CVE-2024-38477	Apache HTTP サーバーの mod_proxy モジュールにおける nullポインタの逆参照により、攻撃者は細工された悪意のあるリクエストを介してサーバーをクラッシュさせることができます。
CVE-2024-39573	mod_rewrite における SSRF の潜在的な脆弱性により、攻撃者は安全でない RewriteRules を引き起こし、mod-proxy によって処理される URL を予期せず設定し、意図されたアクセス制御をバイパスする可能性があります。
CVE-2024-40898	サーバ/vhost コンテキストでの mod-rewrite を伴う Windows 上の Apache HTTP サーバにおける SSRF の脆弱性により、巧妙に細工された要求を介して、悪意のあるサーバに NTLM ハッシュが漏洩される可能性があります。
CVE-2025-3891	Apache HTTP サーバの mod_auth_openidc モジュールの欠陥により、リモートの攻撃者は、OIDCPreservePostディレクティブが有効になっている場合に空の POST リクエストを送信して、サービス拒否をトリガーできます。

影響を受けるサードパーティ ソフトウェア コンポーネントを脆弱性の修正が含まれるバージョンにアップグレードする必要があります。製品の今後のバージョンはこの脆弱性の影響を受けません。

欠陥 ID : [CSCws68830](#)

この製品には、次の Common Vulnerabilities および Exposures (CVE) によって識別される脆弱性の影響を受けるサードパーティ ソフトウェアが含まれています。

CVE ID	説明
CVE-2005-3962	Perl 5.8.6 および 5.9.2 のフォーマット文字列機能 (Perl_sv_vcatpvfn) の整数オーバーフローにより、攻撃者は任意のメモリを上書きしたり、大きな値を持つフォーマット文字列指定子を介して任意のコードを実行したりできます。
CVE-2005-4278	Gentoo Linux 上の 5.8.7-r1 より前の Perl における信頼できない検索パスの脆弱性により、Portage グループ内のローカルユーザーが Portage の一時的なビルドディレクトリ内の悪意のある共有オブジェクトを介して権限を取得する可能性があります。
CVE-2007-5116	Perl 5.8 の正規表現エンジン (regcomp.c) のポリモーフィック型イックオPCODEのサポートにおけるバッファオーバーフローにより、コンテキスト依存の攻撃者は、正規表現のバイトを Unicode 文字に切り替えることで任意のコードを実行することが可能になります。
CVE-2010-1158	Perl 5.8.x の正規表現エンジンの整数オーバーフローにより、コンテキスト依存の攻撃者は、巧妙に細工された正規表現を長い文字列と照合することで、サービス拒否 (スタック消費とクラッシュ) を引き起こすことができます。
CVE-2011-2728	5.14.2 より前の Perl の File::Glob モジュールの <code>bsd_glob</code> 関数により、コンテキスト依存の攻撃者は <code>GLOB_ALTDIRFUNC</code> フラグを使用した <code>glob</code> 式を介してサービス拒否 (クラッシュ) を引き起こし、初期化されていないポインタの逆参照をトリガーできます。
CVE-2011-2939	Perl の Encode モジュールの <code>decode_xs</code> 関数の <code>off-by-one</code> エラーにより、コンテキスト依存の攻撃者は、巧妙に細工された Unicode 文字列を介してサービス拒否 (メモリ破損) を引き起こしたり、任意のコードを実行したりできます。
CVE-2012-6329	Perl 5.17.7 より前の <code>Locale::Maketext</code> の実装では、バックスラッシュとメソッド名が適切に処理されないため、コンテキスト依存の攻撃者は、巧妙に細工された変換文字列を介して任意のコマンドを実行できます。
CVE-2013-1667	Perl 5.8.2 ~ 5.16.x の再ハッシュメカニズムにより、コンテキスト依存の攻撃者は、巧妙に細工されたハッシュキーを介してサービス拒否 (メモリ消費とクラッシュ) を引き起こすことができます。
CVE-2014-4330	2.154 より前の <code>Data::Dumper</code> の <code>Dumper</code> メソッドにより、コンテキスト依存の攻撃者が、深くネストされた <code>Array-Reference</code> を介してサービス拒否 (スタックの枯渇とクラッシュ) を引き起こす可能性があります。

CVE ID	説明
CVE-2015-8853	Perl 5.24.0 より前の正規表現エンジンでは、コンテキスト依存の攻撃者が、巧妙に細工された UTF-8 データを介してサービス拒否（無限ループと高い CPU 使用率）を引き起こすことができます。
CVE-2016-1238	Perl 5.x（5.22.3 より前および 5.24.1）は、モジュール包含パス（@INC）からカレントディレクトリ（「.」）を適切に削除しないため、ローカルユーザは、トロイの木馬モジュールを介して権限を取得できます。
CVE-2016-2381	Perl は、コンテキスト依存の攻撃者が、envp 配列の重複した環境変数を使用し、子プロセスの汚染保護メカニズムをバイパスさせる可能性があります。
CVE-2017-12814	Windows の 5.24.3-RC1 より前の 5.26.x および 5.26.1-RC1 より前の Perl の CPerlHost::Add メソッドの CPerlHost::Add メソッドにより、攻撃者が長い環境変数を介して任意のコードを実行できるを参照してください。
CVE-2017-12837	5.24.3-RC1 より前、および 5.26.1-RC1 より前の 5.26.x の Perl における、regcomp.c 内の S_regatom 関数には、ヒープベースのバッファオーバーフローの脆弱性のため、リモートの攻撃者は、\N{} エスケープと、case-insensitive 修飾子を含む正規表現を用いて、サービス拒否状態を引き起こす可能性があります。
CVE-2017-12883	5.24.3-RC1 より前、および 5.26.1-RC1 より前の 5.26.x の Perl における、regcomp.c の S_grok_bslash_N 関数のバッファオーバーフローにより、リモートの攻撃者は、無効な \N{U+...} エスケープを含む巧妙に細工された正規表現を用いて、機密情報を開示したり、サービス拒否状態を引き起こす可能性があります。
CVE-2018-12015	Perl 5.26.2 までの Archive::Tar モジュールのため、リモートの攻撃者はディレクトリ トラバーサル保護をバイパスし、シンボリックリンクと同じ名前の通常のファイルを含むアーカイブを介して任意のファイルを上書きできます。
CVE-2018-18311	Perl 5.26.3 および 5.28.1 より前の Perl_my_setenv 関数の整数オーバーフローにより、ローカルの攻撃者がサービス拒否を引き起こしたり、大きな環境変数を介して任意のコードを実行したりできる。
CVE-2018-18312	Perl 5.26.3 および 5.28.1 より前の regcomp.c の S_handle_regex_sets 関数におけるヒープベースのバッファオーバーフローにより、リモートの攻撃者がサービス拒否を引き起こしたり、巧妙に細工された正規表現を介して任意のコードを実行したりできるようになります。

CVE ID	説明
CVE-2018-18313	Perl 5.26.3 および 5.28.1 より前の <code>regcomp.c</code> の <code>S_grok_bslash_N</code> 関数によるヒープベースのバッファ読み取りオーバーフローにより、リモート攻撃者が巧妙に細工された正規表現を介してプロセスメモリから機密情報を開示できるようになります。
CVE-2018-18314	Perl 5.26.3 および 5.28.1 より前の <code>regcomp.c</code> の <code>S_regtom</code> 関数でのヒープベースのバッファオーバーフローにより、リモートの攻撃者がサービス拒否を引き起こしたり、巧妙に細工された正規表現を介して任意のコードを実行したりできるようになります。
CVE-2018-6913	Perl 5.26.2 より前の <code>pack</code> 関数のヒープベースのバッファオーバーフローにより、コンテキスト依存の攻撃者は、大きな項目数を介して任意のコードを実行できるようになります。
CVE-2020-10543	Perl 5.30.3 より前の 32 ビットプラットフォームでは、ネストされた正規表現修飾子に整数オーバーフローがあるため、ヒープベースのバッファオーバーフローが発生します。
CVE-2020-10878	5.30.3 より前の Perl には、正規表現エンジンでの特定の命令の誤った処理に関連する整数オーバーフローがあり、命令インジェクションにつながる可能性があります。
CVE-2020-12723	Perl 5.30.3 より前の正規表現コンパイラ (<code>regcomp.c</code>) では、 <code>S_study_chunk</code> の再帰的呼び出し中に、バッファオーバーフローの脆弱性が発生します。
CVE-2022-48522	警告メッセージを出力しようとする、Perl 5.34.0 の <code>S_find_uninit_var</code> 関数のスタックベースのクラッシュ（無限再帰）が発生し、サービス拒否につながる可能性があります。
CVE-2023-31484	CPAN.pm (2.35 より前) および Perl (5.38.0 より前) は、HTTPS を介してディストリビューションをダウンロードするときに TLS 証明書を検証しないため、ユーザが中間者攻撃にさらされます。
CVE-2023-31486	Perl のコアモジュールである HTTP::Tiny の 0.083 より前には、安全でないデフォルト TLS 設定があつて、ユーザが証明書の検証をオプトインする必要があり、そのためアプリケーションが中間者攻撃にさらされる可能性があります。
CVE-2023-47039	Windows の Perl には、バイナリハイジャックの脆弱性があります。これは、システムパスに依存してシェル (<code>cmd.exe</code>) を見つけ、まず現在の作業ディレクトリを検索して、ローカル特権昇格を許可するために発生します。

影響を受けるサードパーティソフトウェアコンポーネントを脆弱性の修正が含まれるバージョンにアップグレードする必要があります。製品の今後のバージョンはこの脆弱性の影響を受けません。

XE シリーズ M8 サーバファームウェア リリース 6.0(1.260001) のセキュリティ修正：なし

C シリーズ M8 サーバファームウェア リリース 6.0(1.250194) のセキュリティ修正：なし

Cisco UCS X シリーズ M8、M7 6.0(1.252114)、M6、B シリーズ M6 6.0(1.250179)、M5 6.0(1.250169) および C シリーズ M8、M7、M6 6.0(1.250192) サーバファームウェア リリースでセキュリティ修正：なし

XE シリーズ M8 6.0(1.251030) サーバファームウェア リリースのセキュリティ修正：なし

X シリーズ M8 サーバファームウェア リリース 6.0(1.252039) のセキュリティ修正：なし

C シリーズ M8、M7、M6 6.0(1.250174) サーバファームウェア リリースのセキュリティ修正

このセクションでは、セキュリティ修正について簡単に説明します。

不具合 ID - CSCwq36167

Cisco UCS C-Series M6 ラック サーバーは、次の一般的な脆弱性およびエクスポージャ（CVE）ID によって特定された脆弱性の影響を受けるインテル CPU を搭載しています：

- **CVE-2025-20067**：一部の Intel（R）CSME および Intel（R）SPS ファームウェアに観察可能なタイミングの不一致があるため、特権ユーザーがローカルアクセスを介して特権のエスカレーションを有効にできる可能性があります。

影響を受けるサードパーティ ソフトウェア コンポーネントを脆弱性の修正が含まれるバージョンにアップグレードする必要があります。製品の今後のバージョンはこの脆弱性の影響を受けません。

不具合 ID - CSCwq36171

Cisco UCS C-Series M7 ラック サーバーは、次の一般的な脆弱性およびエクスポージャ（CVE）ID によって特定された脆弱性の影響を受けるインテル CPU を搭載しています。

- **CVE-2025-21096**：一部の Intel（R）TDX のファームウェアの不適切なバッファ制御により、権限ユーザーがローカルアクセスを介して権限のエスカレーションを有効にできる可能性があります。
- **CVE-2025-20053**：一部の Intel（R）Xeon（R）プロセッサの SGX 対応ファームウェアの不適切なバッファ制御により、特権ユーザーがローカルアクセスを介して特権のエスカレーションを有効にできる可能性があります。
- **CVE-2025-24305**：一部の Intel（R）Xeon（R）プロセッサの Alias Checking Trusted Module（ACTM）ファームウェアの制御フロー管理が不十分なため、特権ユーザーがローカルアクセスを介して特権のエスカレーションを有効にできる可能性があります。
- **CVE-2025-20613**：一部の Intel（R）TDX 向けファームウェアの疑似乱数生成器（PRNG）の予測シードで、認証されたユーザーがローカルアクセスを介した情報開示を有効にする可能性があります。
- **CVE-2025-21090**：一部の Intel（R）Xeon（R）プロセッサにアクティブに割り当てられたリソースへの参照が見つからない場合、認証されたユーザーがローカルアクセスを介してサービス拒否を有効にする可能性があります。
- **CVE-2025-22853**：一部の Intel（R）TDX のファームウェアの不適切な同期により、特権ユーザーがローカルアクセスを介して特権のエスカレーションを有効にできる可能性があります。

影響を受けるサードパーティ ソフトウェア コンポーネントを脆弱性の修正が含まれるバージョンにアップグレードする必要があります。製品の今後のバージョンはこの脆弱性の影響を受けません。

Cisco UCS X シリーズ M8、M7、M6 6.0(1.250122)、B シリーズ M6、M5 6.0(1.250127) および C シリーズ M8、M7、M6 6.0(1.250131) サーバー ファームウェア リリース：なし

Cisco UCS X シリーズ M8、M7、M6 6.0(1.250120)、B シリーズ M6、M5 6.0(1.250126) および C シリーズ M8、M7、M6 6.0(1.250127) サーバー ファームウェア リリース

このセクションでは、セキュリティ修正について簡単に説明します。

不具合 ID - CSCwm98102

Cisco UCS B シリーズ ブレード サーバー、UCS C シリーズ ラック サーバー、UCS X シリーズ コンピューティング ノードには、以下の共通脆弱性識別子 (CVE) ID で識別される脆弱性の影響を受ける、オプションの Trusted Platform Module (TPM) 2.0 が含まれています：

- **CVE-2025-2884** : TCG TPM2.0 リファレンスの実装の CryptHmacSign ヘルパー関数は、署名キーのアルゴリズムで署名スキームの検証が不足しているため、境界外読み取りに対して脆弱です。TCG 標準規格 TPM2.0 については、エラッタ リビジョン 1.83 およびアドバイザリ TCGVRT0009 を参照してください。

Cisco UCS サーバーには、次のオプション TPM モジュールのいずれかが搭載されています。

- UCSX-TPM2-002
- UCSX-TPM-002C
- UCS-TPM-002D
- UCSX-TPM-002D

影響を受けるサードパーティ ソフトウェア コンポーネントを脆弱性の修正が含まれるバージョンにアップグレードする必要があります。製品の今後のバージョンはこの脆弱性の影響を受けません。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。