■新機能
●アップグレードする前に知っておくべき重要な点
・SSL VPN 互換性について
　このバージョンでは、OpenVPN が 2.6.0 にアップグレードされました。 当バージョンにアップグレードされたVCRは、次のクライアントおよび VCROS バージョンでは SSL VPN トンネルを確立できません。
　・VCROS 18.5 以前のバージョン: VCROS 18.5 以前のバージョンと当バージョンの間では、サイト間 SSL VPN は確立されません。両方のVCRを同時にアップグレードすることをお勧めします。あるいは、サイト間の IPsec を使用することもできます。
　・レガシー SSL VPN クライアント: リモート アクセス SSL VPN トンネルは、レガシー SSL VPN クライアントでは確立されません。 Sophos Connect クライアントまたは OpenVPN クライアントなどのサードパーティ クライアントを使用することも、リモート アクセス IPsec トンネルを使用することもできます。

●重要なセキュリティ強化
このリリースでは、VCRを攻撃から保護するのに役立つ 2 つのセキュリティ拡張機能が実装されています。
これらの変更は、WAN ゾーンから Web 管理コンソールおよびユーザー ポータルへのアクセスに影響します。

・特定の WAN IP アドレスからの Web 管理コンソール アクセス:
　ブルート フォース攻撃や偵察攻撃の可能性を減らすために、すべての WAN ソース（インターネット全体）からの Web 管理コンソール アクセスをオフにすることを強くお勧めします。
　WAN から Web 管理コンソールへのアクセスを提供する必要がある場合は、[管理] > [デバイス アクセス] に移動し、ローカル サービス ACL 例外ルールを追加して、特定の IP アドレスとネットワークを許可します。
　Web 管理コンソールは、すべての WAN ソースから利用できなくなります。そのため、[管理] > [デバイス アクセス] の [HTTPS] で WAN を選択することはできません。
　注: 既存の展開は影響を受けません。すべての WAN ソースからの Web 管理コンソール アクセスをすでに有効にしている場合、アップグレードした後も引き続き動作します。

・Web 管理コンソールおよびユーザー ポータルへの未使用の WAN アクセス:
　90 日間連続して WAN ゾーンからのサインインが成功しなかった場合、すべての WAN ソースからの Web 管理コンソールとユーザー ポータルのアクセスがオフになります。これはすべての展開に当てはまります。
　ローカル サービス ACL 例外ルールを通じて特定の WAN IP アドレスおよびネットワークに与えられたアクセスは影響を受けません。これらのソースは、サインインがない場合でも引き続きアクセスできます。
　これは、アクセスがオンになっているにもかかわらず使用されず、VCRがインターネット上でブルート フォース攻撃や偵察攻撃にさらされる可能性があるインスタンスを防ぐために行われています。
　注: 移行前にすでに有効にしていて、積極的に使用している場合は、機能は引き続き動

作します。

●VPN の機能強化
・OpenVPN 3.0: VCR は OpenVPN 3.0 クライアントと互換性を持つようになりました。ユーザーは、VPN ポータルから互換性のある構成ファイルをダウンロードできます。
・システム生成のトラフィック: CLI コマンドを使用すると、リモート サブネットが [Any] に設定されている場合に、システム生成のトラフィックがポリシーベースの IPsec トンネルを通過するのを防ぐことができます。
・StrongSwan バージョン 5.9.11 を使用するようになりました。
・VPN ポータル: リモート アクセス VPN ユーザーは、新しく強化された安全性の高いコンテナ化されたセルフサービス VPN ポータルを利用できます。これには、Sophos Connect クライアントや設定などのリモート アクセスのダウンロードが含まれており、リモート アクセス VPN 接続の自動プロビジョニングを実行します。クライアントレス VPN ブックマークも含まれています。
・これらのサービスはユーザー ポータルでは利用できなくなり、ユーザー ポータルを WAN に公開する必要性が最小限に抑えられ、そのセキュリティが強化されます。互換性を維持するために、VPN ポータルはデフォルトで以前のユーザー ポータル ポート (443) で利用可能です。 WAF または SSL VPN と共通のポートを共有できます。ユーザー ポータルはデフォルトでポート 4443 を使用するようになりました。
・SSL VPN の FQDN: 完全修飾ドメイン名 (FQDN) ホストおよびグループのサポートは、リモート アクセスおよびサイト間 SSL VPN で利用できます。これらは、許可されたローカル ネットワークおよびリモート ネットワークで選択できます。
・IPsec VPN:
IPsec VPN のフェーズ 1 IKEv2 トンネルは、GCM およびスイート B 暗号をサポートします。フェーズ 2 IKEv2 トンネルはすでにこれらの暗号を提供しており、より強力な暗号化の完全な配信を保証します。
ルートベース VPN の複数のリモート ゲートウェイのサポート: ルートベース VPN では、リモート ゲートウェイのワイルドカード アドレス (*) を入力できます。これにより、動的ゲートウェイ IP 展開での明示的な DDNS または FQDN 構成が不要になります。
固有の事前共有キー: IKEv2 プロファイルを使用し、ローカル ID とリモート ID の一意のセットを構成する場合、同じローカルおよびリモート ゲートウェイ設定で VPN 接続に固有の事前共有キー (PSK) を使用できます。
DH グループ 27 ～ 30: DH グループ 27 ～ 30 は、RFC 6954 に基づく IKEv2 IPsec プロファイルに使用できます。

●アクティブな脅威対応
・Sophos X-Ops 脅威フィード: Advanced Threat Protection の名前が Sophos X-Ops 脅威フィードに変更されました。 SophosLabs からの脅威フィードの定期的な更新を提供します。

●分散型企業向けのネットワークの拡張性と回復力
・IPv6 DHCP プレフィックス委任と BGP、SD-WAN

IPv6 DHCP プレフィックス委任: 内部ネットワーク用の ISP による DHCP プレフィックス委任とのシームレスな統合。これにより、内部サブネットへの IPv6 プレフィックスの割り当てが自動化され、ネットワークのセットアップが簡素化され、手動構成が削減されます。

BGP IPv6: 動的ルーティング エンジンの機能強化により、IPv6 の相互運用性が向上するために BGPv6 がサポートされるようになりました。

SD-WAN のスケーラビリティ: SD-WAN ゲートウェイのスケーラビリティが 3 倍の 3,072 ゲートウェイ、SD-WAN プロファイルの数が 1,024 に増加しました。

●UIの機能強化

・インターフェースをオンまたはオフにする: 構成を保持しながらインターフェースをオンまたはオフにします。コントロールセンターにオフの状態が表示されます。

エイリアスまたはトンネル インターフェース、および LAG またはブリッジ インターフェースのメンバーをオフにすることはできませんが、LAG またはブリッジ インターフェース全体をオフにすることはできます。

・オブジェクト参照ルックアップ: すべてのホストおよびサービス オブジェクトの使用数と、ルール、ポリシー、ルートなど、オブジェクトが使用されているすべての場所のリストを確認できます。さまざまな場所に行かなくても、オブジェクト リストからオブジェクトを編集したり削除したりできます。

・Web 管理コンソールの高解像度: Web 管理コンソールは高解像度ディスプレイを使用し、スケーラブルなユーザー インターフェースを提供するようになりました。表はフル HD 幅（1920 ピクセル）を使用してより多くの情報を表示し、水平方向にスクロールする必要性を減らします。

・失敗したファームウェア更新の自動ロールバック: ファームウェアのアップグレードを完了できない場合、自動的に以前のファームウェア バージョンにロールバックされます。コントロール センターにアラートが表示されます。

・Microsoft Entra ID（Azure AD）SSO:

キャプティブ ポータル: Microsoft Entra ID（Azure AD）SSO は、キャプティブ ポータルを介したユーザー認証をサポートするようになりました。Web 管理コンソールに Azure AD SSO 認証が追加されました。

グループのインポート: 新しいインポート アシスタントを使用して、すべての Microsoft Entra ID（Azure AD）グループ、または Azure Portal から指定した属性に一致するグループをインポートできます。これにより、VCR内にグループを手動で作成する必要がなくなります。

自動 Azure RBAC: ロールベースのアクセス制御（RBAC）を導入します。 Azure Portal でユーザーのロールを変更すると、次回のサインイン時にVCRによって新しいロールが自動的に適用されます。また、新しいロールに適用されるプロファイルと権限も適用されます。

●デバイスアクセスとローカルサービスACL例外ルール

デバイス アクセス: このリリースでは、ゾーンから特定のサービスにアクセスするためのデバイス アクセス グリッドが強化されています。グリッドもグループ化されており、直感的な構成と詳細な制御が可能です。

・IPsec: IPsec サービスは、ゾーンに基づいてトラフィックを許可またはブロックするデバイス アクセスで利用できます。
・VPN サービス: IPsec、SSL VPN、VPN ポータルは、VPN サービスの下にグループ化されています。
ローカル サービス ACL 例外ルール:
・リスト ビュー: 例外ルールのリスト ビューでは、ソース、宛先、サービス、アクションなどの詳細情報が提供され、ルールが完全に表示されるため、ルールを開いて情報を確認する必要がなくなります。
・サービス: デバイス アクセス グリッド内のすべてのサービスは、IPsec サービスなど、例外ルールのサービスで利用できるようになり、きめ細かい制御が可能になります。たとえば、WAN からのサービスが許可されている場合に、特定のインターフェースで VPN を許可またはブロックする例外ルールを作成できます。国と IP アドレスを指定して、中国などの特定の国からの VPN リクエストをドロップしたり、既知の FQDN からの VPN トラフィックを許可したりすることもできます。例外ルールで利用できる追加サービスは、AD SSO、RADIUS SSO、キャプティブ ポータル、クライアント認証、Chromebook、ワイヤレス、SMTP、SNMP、および IPsec です。
・追加のオブジェクト タイプ: オブジェクト タイプ、FQDN ホスト、FQDN ホスト グループ、MAC アドレス、および MAC アドレス リストを送信元ホストと宛先ホストで選択できるため、ローカル ACL 例外ルールで動的 IP アドレスを更新する必要がなくなります。

●DHCP の拡張機能
・DHCP リース時間: リース間隔のハーフタイムが 30 秒以下の場合、DHCP クライアントは 30 秒で更新要求を行い、継続的な WAN 接続を確保します。
・ブート オプション: DHCP は、DHCP ヘッダーでブート サーバーとブート ファイルのオプションをサポートするようになりました。特定の DHCP オプションを介してパラメータを送信し続けて、ネットワーク デバイスをプロビジョニングすることもできます。

●ロギングの機能強化
・ログ ファイルのダウンロード: Web 管理コンソールの [診断] ページの [トラブルシューティング ログ] から個々のログ ファイルをダウンロードできます。統合トラブルシューティング レポート (CTR) には、すべてのログ ファイルが引き続き含まれます。
・CTR のデフォルトのログ行: 統合トラブルシューティング レポートのログ ファイルのデフォルトのログ行数は 10,000 になりました。
・Syslog 区切り文字: Syslog イベント メッセージの区切り文字をカスタマイズできるため、ログ データの管理が柔軟になります。

■その他の機能強化
・動的ルーティング: VCRは最大 4,000 のマルチキャスト グループをサポートするようになり、動的ルーティング展開の拡張性が向上しました。これにより、動的ルートがマルチキャスト グループに参加できないことに関連する問題が解消されます。
・Akamai SIA 統合: Akamai Secure Internet Access (SIA) 統合により、ルートベースの IPsec VPN トンネル経由で冗長性と復元力のある SD-WAN を使用して、VCR

から Akamai SIA SSE (Security Service Edge) へのトラフィックをオンランプできます。
・Cloudflare Magic WAN の統合: ルートベースの IPsec VPN または GRE トンネル経由で冗長性と復元力のある SD-WAN を使用して、VCR から CloudFlare Magic WAN へのトラフィックをオンランプできます。
・Web: Web プロキシでは、プロキシの DNS 解決中に宛先 IP アドレスが変更されることで生じる潜在的な脆弱性に対処するために、ファーミング保護機能を改良しました。更新された動作により、ファイアウォール ポリシーは、ファーミング保護からの DNS 解決された IP アドレスを使用して再評価されるようになります。
・ログ: syslog イベント メッセージの区切り文字をカスタマイズできるため、ログ データの管理が柔軟になります。
・新しい SSD ファームウェア: SSD ドライブに対してファームウェアのアップグレードが可能です。
・レポート: /var パーティションがいっぱいになるのを防ぐために、オンボックス レポートのストレージしきい値が 90 パーセントから 80 パーセントに引き下げられました。
・自動言語検出: Web 管理コンソールとユーザー ポータルは、VCRがサポートする言語のうちブラウザーの優先言語を自動的に選択して保存し、シームレスなサインイン エクスペリエンスを提供します。
・カスタム ゲートウェイ: カスタム ゲートウェイはリンクローカル アドレスをサポートするようになりました。
・IPv4 インターネット ホスト グループ: すべてのパブリック IPv4 アドレス範囲を含むようにデフォルトのパブリック IPv4 ホスト範囲を更新しました。
・オブジェクトの説明: IP、MAC、FQDN、およびサービス オブジェクトの説明フィールドを追加しました。
・国リスト: 国リストを更新しました。
・XML API: 当バージョンでは、バージョン 17.5 および 18.0 の XML API バージョンをサポートしません。使用する APIVersion タグが古いバージョンを示している場合は、タグをサポートされている API バージョンに変更します。

■解決された問題
●API Framework
・特殊文字を含む Web カテゴリを含むユーザー アクティビティをインポートできません。

●AppFilter Policy
・Sophos Central からアプリ フィルター ポリシーを更新またはプッシュできません。
・すべてのアプリケーションをブロックするように設定されたアプリケーション フィルタ ポリシーは、Sophos Central 管理を通じて設定された場合にはリスク レベルを設定しません。

●認証
・nsgencode マルチスレッド サポートがないため、access_server が応答を停止します。

・ユーザー名に特殊文字が含まれている場合、AD グループのインポートは失敗します。
・MFA が有効になっている場合、管理者は 2 回間違った試行を行うと、Web 管理コンソールへのアクセスがブロックされます。
・Web プロキシのリスニング ポートが 3128 ではない場合、Azure AD SSO キャプティブ ポータル認証が停止します。
・データ匿名化設定から承認者を削除できません。
・カスタム コードを含むキャプティブ ポータルが正しく動作しません。
・認証に失敗した SSL VPN ユーザーの送信元 IP アドレスがログ ビューアに表示されません。
・セットアップ アシスタントによるファームウェアの更新を必須にすると、初期セットアップが繰り返し開始されます。
・ユーザー ID がマークされていないため、ファイアウォール ルールの既知のユーザーと一致するオプションによりトラフィックがドロップされます。
・MFA 有効化/無効化イベントのログがありません。
・VPN グループに属していない RADIUS ユーザーは、SSL VPN に接続できます。
・管理者が 2 要素認証を有効にし、デフォルトの管理者以外の管理者を使用してサインインした後に追加すると、SSH キーが表示されなくなります。
・静的 IP アドレスは、SSL VPN ユーザーに対して散発的に解放されるわけではありません。
・eDirectory認証サーバーでのトランザクション障害。
・ブルート フォース サインイン イベントのログ メッセージを更新しました。
・管理者が Azure AD SSO 経由でサインインするときに証明書をアップロードすると、サインアウトになります。
・ユーザー名に一重引用符が含まれていると使用状況の表示が機能せず、Web 管理コンソールが応答を停止します。
・AD サーバー接続がフラップすると、ldap_bind が 30 分間ブロックされ、タイムアウトが発生し、新しい認証リクエストが失敗します。
・プライマリ ユーザー グループ ID が 9999 より大きい場合、キャプティブ ポータルはサインイン後 5 ～ 10 秒以内に切断されます。

●バックアップ–リストア
・バックアップのダウンロード ボタンが反応しません。

●証明書
・属性チャレンジ パスワードにより、No–IP で証明書を発行できなくなります。
・[Web] > [一般設定] からデフォルトの証明書をダウンロードできません。管理者がダウンロード ボタンをクリックするとサインアウトします。

●クライアントレスアクセス
・名前にウムラウト文字が含まれている場合、クライアントレス アクセスは機能しません。
・RDP のクライアントレス VPN ブックマークが断続的に停止します。ユーザーをサインアウトします。

・ユーザー名にスペースが含まれている場合、クライアントレス アクセス SSL VPN 経由で RDP に接続できません。
・VNCFreeRDP が応答を停止します。

●CM
・Sophos Central にアラートが表示されます。 「ファイアウォールは過去 5 分間 Sophos Central にチェックインしていません。」
・集中管理を無効にすることは、API ドキュメントに従って機能しません。
・VCRの Web 管理コンソールが Sophos Central ページで応答を停止します。
・Garner スレッドが中央管理プラグインでスタックしました。
・特定の API 呼び出しが機能しません。
・Sophos Central Firewall Management から管理者アカウントのパスワードを変更できません。
・VPN トンネルは、VCRとサードパーティのファイアウォールの間でフラップします。
・Sophos Central メニューに移動した後、Web 管理コンソールが応答しません。

●CM, コアユーティリティ
・libssh2 CVE-2023-48795 の脆弱性を修正しました。

●コアユーティリティ
・NPU ログエラーを修正しました。
・SWAP メモリの使用量がいっぱいです。
・管理者の公開キー認証は、Sophos Central では管理できません。

●DHCP
・DHCP 次のサーバーとブート ファイルは無視されます。PXE ブート DHCP オプション 66 および 67。
・すべてのインターフェースを選択したリレー エージェント要求で構成された DHCP サーバーは、移行またはバックアップの復元後に機能しません。
・DHCP ログの記録を停止し、Garner サービスは応答せず、再起動できません。
・無効なサブネット ID を使用してダウンストリーム インターフェースを作成すると、間違ったエラー メッセージが表示されます。
・委任インターフェース用に自動的に作成された RA サーバーでは、オンリンクおよび自律設定がオフになります。
・静的 MAC アドレスを特定の DHCP プールに追加できません。
・インターフェースを設定または編集できません。

●ダイナミックルーティング (BGP)
・BGP-FRR は、設定されたネットワークが RIB で利用できない場合、そのネットワークをアドバタイズしません。
・実際にはブロードキャスト IP アドレスであるゲートウェイ IP アドレスが構成に含まれている場合、Zebra は継続的に再起動します。

●ダイナミックルーティング (OSPF)

・ICMP エコーを使用した連続スキャンを実行すると、OSPF がフラップを繰り返します。

●ダイナミックルーティング (PIM)
・PIM-SMインターフェーステーブルをクリックすると「経路情報を読み取れません」というエラーが表示されます。
・PIMD サービスが応答しません。

●メール
・スパム対策サービスが応答しません。
・拡張子または MIME ヘッダーでブロックされている場合でも、添付は許可されます。
・DKIM が期待どおりに機能しません。
・隔離ダイジェストで [解放してレポート] をクリックした後、スマートホストを介した電子メール トランスポートは、「Return-Path:」ヘッダーと「From:」ヘッダーにユーザーの 2 つの電子メール アドレスが含まれているため拒否されます。
・送信者のアドレスが例外に追加されている場合でも、メールは隔離されます。
・EmailUtilityis_valid_messageid が厳密すぎます。
・Web サーバー保護ポリシーで AV としてソフォスを使用する場合のエラー ログ。
・電子メール メッセージ ID の検証が厳しすぎる。
・Exim: libspf2 の脆弱性 (CVE-2023-42118)。
・DKIM 検証が失敗したため、特定のドメインからの受信メールが隔離されます。
・マルウェア スキャンが失敗したため、添付ファイル付きの受信メールは配信されません。
・IP アドレスが無効な場合、通知メールでエラーが発生します。
・従来の電子メール モードが頻繁に応答を停止します。
・ゼロデイ保護がオンになっている場合、MIME タイプ認識の問題が発生します。
・SMTP 隔離からの電子メールの表示、解放、削除ができません。
・メールポーラーで時折 UT エラーが発生する。
・リリースリンク設定は隔離ダイジェストに保存できません。
・「スパム スキャンに失敗しました。ローカルのスパム対策に接続できません」というエラーが表示されたスパム メールは許可されます。
・SPX パスワードが平文で公開される (CVE-2023-5552)。
・従来の TLS プロトコルをオフにできません。
・ユーザーは重複した電子メールを受信します。

●ファイアウォール
・許可された子接続はドロップされたとしてログに記録されます。
・FIN_WAIT ステータスのソケットの数が多いため、接続が失敗します。
・アップグレード後、デバイスはフェールセーフ モードになります。ファイアウォール フレームワークを適用できません。
・Entities.xml には、Web 管理コンソールには表示されないファイアウォール ルールが表示されます。
・VCRが自動的に再起動します (RIP 0010muser_match+0x747)。
・ファイアウォール ルールの作成に使用した XML API の障害により、バックアップと復

元後にファイアウォール ルールが機能しなくなりました。
・名前にバックスラッシュ文字が含まれている場合、ローカル ACL は機能しません。
・Logviewer は、IPv6 ヘアピン NAT の dst_trans_ip フィールドに送信元 IPv6 アドレスを表示します。
・MAC フィルターのスプーフィング チェックが機能しません。 SPOOF_CHECK チェーン エントリがありません。
・VCRの再起動後に NAT ルールがマークされない
・Pktcapd bpf フィルターにより補助が再起動されます。
・デバイスの再起動を引き起こす Pktcapd bpf フィルター (___bpf_prog_run)。
・VCROS は、別のネットワークからのネットワーク IP アドレスおよびブロードキャスト IP アドレスの要求にアクセスできます。

●ファイアウォール、SDWAN ルーティング
・SD-WAN ポリシーが適用されると、静的マルチキャスト パケットは応答先を変更します。

●FQDN
・低い TTL (2 ～ 5 秒) で FQDN を解決すると、ワイルドカード FQDN ホストで問題が発生します。
・非 VCROS DNS サーバーがクライアントに設定されている場合、サブドメイン学習は機能しません。
・新しい FQDN ホスト オブジェクトをVCRに追加すると、リゾルバーが再起動するか応答しなくなり、その間に DNS 解決が失敗します。

●ゲートウェイ管理
・wwan-gwid がそのモニター ID と同じでない場合、WWAN ゲートウェイ更新フローは間違ったモニター ID を更新します。
・WAN リンク マネージャーでフェイルオーバー ルールを更新中にエラーが発生しました。
・DGD サービスは停電後に停止し、再起動しませんでした。

●ハードウェア
・デバイスへのアクセスが失われ、ログは利用できなくなります。

●ホットスポット
・ユーザー用に作成されたホットスポット バウチャーに情報がありません。
・ホットスポット サインインの時間がローカル システム時間ではなく UTC で表示されるまで有効です。
・ホットスポット バウチャーのユーザー ポータルで並べ替え機能が正しく動作しません。

●インターフェース管理
・VCRが応答を停止したため、再起動が必要になります。
・Web 管理コンソールの言語がドイツ語に設定されている場合、Port1 をオフにできませ

ん。
・ブリッジ インターフェースを削除または変更できません。
・MAC アドレス フィルタリングにおける大文字と小文字の不一致。

●IPS
・IPS ログはログ ビューアでは生成されません。
・IPS シグネチャは、検出された SID をブロックしませんでした。
・Sophos Central 管理を通じて設定した場合の IPS ポリシーの動作の問題。
・IPS ポリシーが期待どおりに機能しないことがある。
・読み取り専用管理者プロファイルの IPS を使用したファイアウォール ルールに関連するカウントの問題。
・注入バッファリークによりトラフィック停止が発生します。
・FIN および RESET パケットは、LAN IP アドレス情報とともに WAN インターフェースから出ます。
・スレッド停止の順序が間違っているため、DAQ シャットダウン中にコアダンプが発生します。
・Snort では CPU 使用率が高く、その結果、帯域幅が低下します。
・RX が小さい場合、証明書ベースの認証がサーバーに失敗します。
・DPI がオンの場合、VCRは LAN 間通信でリセット パケットをドロップします。
・一部のサーバーからの TLS 検査トラフィックのダウンロード速度が遅くなります。
・VCRがロックアップします。 Snortコアが生成されました。
・大規模な初期 rxwin が存在する場合に TLS が復号化されていない場合でも、SSL/TLS インスペクションが有効になっているとダウンロード速度が遅くなります。

●IPsec
・IPsec SA の確立が散発的に中断されます。
・IPsec VPN パスの MTU 関連の IPsec アクセラレーションに関する接続の問題。
・サイト間 VPN とルートベース VPN の両方が同じローカル – リモート ゲートウェイ ペア上で同時に稼働している場合、XFRM トンネルは無効のままになります。
・SSL/TLS インスペクションは VPN ユーザーに対して機能しません。
・トラフィック セレクタが使用されていると、IPsec RBVPN 経由で GUI にアクセスできません。

●IPsec と SDWAN ルーティング
・ブランチ オフィスのユーザーが電子メールを受信できない、後で電子メールを受信する、または IPsec トラフィックが遅くなる。

●L2TP
・L2TP メンバーの最初の行にはチェックボックスは表示されません。

●LCD フレームワーク
・特定のインターフェース オペコードは、csc がデバッグ モードでない場合でも、常にデバッグを有効にして呼び出されます。

●ライセンス

・ライセンス同期の問題により、Web 管理コンソールにアクセスできません。
・ライセンスが同期していません。

●ロギングフレームワーク
・中央レポートが有効になっているログは、127.0.0.1 にある到達不能な syslog サーバーに送信されます。
・ネットワーク トラフィック レポートの計算では、時間ごとに異なる値が表示されます。
・Syslog 形式 数値と文字列の両方としてキー log_id を使用する標準 Syslog プロトコルのログ。
・WAN インターフェース グラフに、時間制限の 5 分前または後に収集された履歴データの誤った値が表示されます。
・AirGap サイトでパターン ファイルを更新できません。
・デバイス上のログ記録が停止します。データベースのディスクイメージの形式が正しくありません。
・ライブ ログはログ ビューアで生成されません。
・Garner は同期キャッシュ中に init_cache_tree で応答を停止します。
・データベース ディスク イメージの形式が不正であるというエラーにより、デバイスでのログ記録が停止しました。
・VCROS が非常に低い速度で Sophos Central にレポートを送信しているため、Central Report ハブにはVCRからの過去 24 時間の統計が表示されません。
・ファイルが 7200 個を超えると、Sophos Central へのファイルの送信がエラーで停止します。

●nSXLd
・「invalid traveller type」エラーを修正しました。
・ドメインの末尾にピリオドを追加すると、Web ポリシーがバイパスされます。
・インターネットがダウンし、「nSXLd SXL サーバーへの接続中に接続タイムアウト」というエラーが発生しました。
・Sophos Central から削除されたポリシーは引き続きVCR側で表示されます。

●PPPoE
・スケジュールされた PPPoE 再接続が機能しません。
・PPPoE ログがありません。

●レポート
・セキュリティ監査レポートのスコア データは、VCRで表示されるものと電子メール経由で受信されるものでは異なります。

●SDWAN ルーティング
・ファイアウォール ルールが一致しない場合があります。
・SD-WAN ルートとデフォルト MASQ は、ポリシーベースの IPsec VPN のシステム生成トラフィックに適用されます。
・インポートとエクスポートには、SD-WAN プロファイルの変更は反映されません。

・garner.log には、キャッシュ障害に関する継続的なログが大量に記録されます。
・SD-WAN ルートおよびプロファイルで IPsec ルートベースの VPN を使用する場合の接続の問題。

●SSLVPN
・ルートベースの VPN 接続の Web 管理コンソールで文法エラーが発生しました。
・カスタム証明書が使用されている場合、tblsslvpnglobalconf に server_dn がないため、.ovpn ファイルを生成できません。
・一部の AD ユーザーは、ユーザー ポータルから SSL VPN 構成ファイルをダウンロードできません。
・特殊文字はエンコードされた値に置き換えられます。
・.ovpn ファイル内の証明書がアップグレード前よりも増加しました。
・SSL VPN リモート アクセス リソースにアクセスできなくなります。
・/conf/certificate/openvpn ディレクトリがありません。
・serveruser.conf ファイルがないため、サイト間の SSL VPN 接続が失敗します。
・ログイン セキュリティ ブロックは管理者にのみ適用され、ユーザーには適用されません。
・SSL VPN サーバーのルート クォータに達しました。
・トンネルは稼働しているにもかかわらず、トラフィックがサイト間 SSL VPN トンネルを通過しません。
・Android/IOS ユーザーは、SSL VPN ovpn ファイルをインポートできません。
・LAN から静的 SSL VPN IP アドレスへの接続は、デバイス上の WAN 経由でルーティングされます。
・認証方法として Azure AD が選択されている場合、サービス ページが応答しなくなります。

●スタティックルーティング
・スタティック ルート設定では、インターフェース IP アドレスをゲートウェイ IP アドレスとして設定できないようにする必要があります。
・PPPoE インターフェースを使用して Web 管理コンソールからルートが設定されている場合、19.0 および 18.5 から 19.5 への移行がブロックされます。

●Synchronized App コントロール
・Garner ログに「usercache_output: notsolve appcatid 0」が記録される。

●UI フレームワーク
・SD-WAN プロファイルの UX の問題。
・バックアップ ファイル名のプレフィックスに & が含まれる場合、バックアップの復元に失敗しました。
・Web 管理コンソールが応答を停止します。
・ユーザー ポータルでの HTTP ホスト ヘッダー インジェクションを修正しました。
・ファイル「.eslintignore」は UI からアクセスできます。
・[管理] > [読み取り専用プロファイル サインインによるデバイス アクセス] で設定を表示できませんでした。

・Package.json URL は SSL VPN ポータルで機能します。

●WAF
・コアダンプにより、WAF が 1 日に数回停止します。
・XML API に WAF パラメータがありません。
・証明書を更新した後、WAF ルールを更新できません。
・Web 管理コンソールでの WAF 保護ポリシーの表示の問題。
・/tmp ディレクトリではファイルが削除されず、スペースが不足し、AV スキャンが失敗します。
・Sophos Central から取得したバックアップを復元できません。

●Web
・カスタム カテゴリからすべてのドメインまたはキーワードを削除しても機能しません。
・「ブロックされた Web 試行」で適切な「Web アクティビティ カテゴリ」レポートを取得できません。
・nasm が実行されていない場合、awarrenhttp は起動しません。
・拡張子 .hpi のファイルをダウンロードするとネットワークが停止します。
・awarrenhttp は、タイムアウト後に nSXLD に再接続する必要があります。
・スレッドが解放されていないため、パターンの更新後に AVD が応答を停止します。
・管理者のアカウントの OTP を有効にできませんでした。
・Web ポリシーが [警告] に設定され、ファイル タイプ ポリシーとデフォルトのアクションが [ブロック] に設定されているため、ページ ブロックが発生します。

●WebInSnort
・WebInSnort は、RSA キー サイズ 3072 を key_param="RSA 不明なタイプ" としてログ ビューアに記録します。

●ワイヤレス
・アクセス ポイント グループにワイヤレス ネットワークを追加した後、Hostapd サービスが停止しました。
・既存のワイヤレス ネットワーク設定から SSID 暗号化を削除した後でも、ホットスポット バウチャーには SSID WLAN パスワードが表示されます。
・更新後、別のゾーンの SSID の「ageing_time」パラメータは 0 にリセットされます。

●WWAN
・Sierra Wireless MC7430 Qualcomm® Snapdragon™ X7 LTE-A が接続されません。