■新機能
●MTA
・MTAモードでのバルクメール: SASIでスパムキャッチ率を強化しました。ファイアウォールは、MTAモードで一括メール設定を提供するようになりました。

●Xstreamアーキテクチャ
・SD-WAN:
 - 今までの4倍の数のSD-WANプロファイルを構成でき、拡張された展開をサポートします。
 - ゲートウェイ管理の改善。ステータス、IPアドレス、インターフェイス、およびヘルスチェックに基づいてゲートウェイをフィルタリングできます。
 - [診断] > [SD-WANパフォーマンス] でSD-WANプロファイルを名前で検索します。
 - SD-WAN負荷分散により、複数のリンクで帯域幅の使用を最大化します。SD-WANプロファイルのルーティング戦略として負荷分散を選択できます。送信元と宛先のIPアドレス、およびゲートウェイの重みとSLAを使用した接続基準に基づいて、ラウンドロビンとセッションの永続性を使用できます。MPLS、WAN、VPN、REDなどの複数のリンクを介したアプリケーショントラフィックのルーティングを保証します。
 - SD-WANプロファイルの強化されたゲートウェイパフォーマンス診断によるリアルタイムの監視とロギング。合計接続数とデータ転送数でリンクパフォーマンスを表示します。トラブルシューティングのためにカウントをリセットすることもできます。SD-WANパフォーマンス診断のヘルプを参照してください。
・IPsecVPN:
 - サポートされる同時トンネルの最大数が4,650から10,000に増加しました。

●動的ルーティング
・OSPFv3:
 - OSPFv3プロトコルをサポートし、IPv6トラフィックの動的ルーティングを有効にします。
・より良いルーティング決定
 - OSPFとOSPFv3は、構成されたインターフェイス速度を使用して、ルーティング用により高速なインターフェイスを選択します。
・BGP
 - BGPの自動ルーターID選択により、ルーターIDの動的更新が可能になります。
・ログ
 - BGP、OSPF、およびOSPFv3の隣接情報に関連するログを提供します。BGPおよびOSPFコマンドのヘルプを参照してください。
・その他の機能強化は次のとおりです。
 - 安定した将来に備えた機能のために、新しいダイナミックルーティングエンジンを統合しました。
 - 他のベンダーとの完全な相互運用性。

●スタティックルート
IPv4スタティックルートのアドミニストレーティブディスタンスとメトリックを設定できます。

●ルーティング動作の重要な変更
ファイアウォールがインターフェイスリンクのステータスとネットワーク構成を監視できるようにする新しいルーティングエンジンを導入しました。以前の動作からの変更点は次のとおりです。
・BGP、OSPF、RIP構成は、デフォルトで、インターフェイスリンクステータスがダウンの場合、ピアへのネットワークとルートの配布を防ぎます。BGPのみのこのデフォルトを変更するには、BGP CLIコンソールで次のコマンドを実行します: no bgp network import-check
・VCROSとBGPネットワークのサブネットが一致しない場合、BGP構成はデフォルトで、ピアへのネットワークとルートの配布を防ぎます。デフォルトを変更するには、BGP CLIコンソールで次のコマンドを実行します: no bgp network import-check
・新しいダイナミックルーティングエンジンのため、Zebra Advanced Shell CLIは使用できません。[Routing] > [Static routes]のVCROS Web管理コンソールで同じ設定を追加できます。

●Quality of life enhancements
・Azure AD SSO
 - Web管理コンソールにサインインするための Azure AD SSO構成をサポートします。
・検索
 - ホストとサービスのデフォルトオブジェクトとカスタムオブジェクトの名前、タイプ、値による検索機能。

・ログストレージ
 - 単一または複数のログファイルのタイムスタンプとサイズの変更に加えて、構成可能なローテーションカウントとアーカイブによりトラブルシューティングを改善するための強化された.logファイルストレージ。

●その他の変更
[Web] > [一般設定] > [Webコンテンツのキャッシュ] の [ソフォスエンドポイントの更新を常にキャッシュする] 設定は削除されました。

■機能強化
Xstream SD-WAN
 - SD-WANルート管理の機能強化。SD-WANルートを既存のルートの上または下に複製し、ルートをリストの任意の位置に移動し、リストの上部または下部にルートを作成できます。
バックアップ管理
 - ファームウェアのバージョンは、バージョンの識別に役立つように、バックアップファイルの名前に含まれています。

■解決された問題
●コアユーティリティIPsec
- .scxファイルにcacertがありません。

●FQDN
- クライアントにVCROS以外のDNSサーバーが設定されている場合、サブドメインの学習が機能しません。

●APIフレームワーク
- Web管理コンソールの複数の認証後SQLi脆弱性を解決しました(CVE-2022-1807)。

●APIフレームワーク、UIフレームワーク
- マルチパートリクエストのフロントエンド検証をフックする必要があります。
- 認証後のコードインジェクション(CVE-2022-3696)。
- 事前認証コードインジェクション(CVE-2022-3236)。

●AppFilterポリシー
- アプリケーションフィルターポリシーをエクスポートできません。
- AppFilterPolicyDetailEdit.jsのDOMベースのXSS。

●認証
- MFAの有効化と無効化のイベントログがありません。
- セットアップウィザードでパスワードを公開します。
- ログビューアに、認証されたSSLVPNユーザーのソースIPフィールド情報が表示されません。
- グループのインポートウィザードに保存されたXSS(CVE-2022-3709)。
- 名前にアポストロフィを含むグループをインポートできません。
- Azure MFAでPUSHを使用して認証できません。
- Web管理コンソールのSSOにより、言語の選択が妨げられます。
- 古いユーザーはライブユーザーリストから削除されません。
- ADが静的ルートを介してアクセスされる場合、アプライアンスが再起動すると、アクセスサーバーが再起動されるまで、STAS認証が機能しなくなります。
- 同じメールアドレス(Azure AD)を持つユーザーを追加できません。

●キャプティブポータル
- カスタムキャプティブポータルでサインインメッセージとサインアウトオプションが表示されない。
- キャプティブポータルのカスタマイズを通じて保存されたXSS(CVE-2022-4238)。

●CDB-CFR
- ファイアウォールで「レポートとログをSophos Centralに送信する」および「設定のバックアップをSophos Centralに送信する」を有効にした後、Sophos CentralからWeb管理コンソールを開くことができません。
- レポートを生成できません。

●証明書
- pfxファイルではCAを使用できませんが、CAアップロードオペコードが呼び出されます。
- 属性チャレンジパスワードにより、No-IPでの証明書の発行が防止されます。

●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。

●CM
- fwcm-eventdエージェントは、SD-WAN接続グループのIPアドレスアップイベントをリッスンしていません。

●CM、UIフレームワーク
- ユーザーポータルのホストインジェクションが報告されました。

●コアユーティリティ

- adminの公開鍵認証は、Sophos Centralでは管理できません。
- セキュリティ監査レポート(SAR)との不一致。
- 同じ執行スケジュール報告書の複製を受け取る。
- OpenSSL(CVE-2022-1292)を介したWeb管理コンソールでの認証後のシェルインジェクションを解決しました。

●DHCP
- DHCP IPリースの問題。
- インターフェイスを構成または編集できません。

●DNS
- kdump:スタックガードページがヒットし、アプライアンスが繰り返し再起動します。

●動的ルーティング(BGP)
- VCROS Web管理コンソールのBGPネットワークは、config-type ciscoの予想されるネットワークではなく、ASCII文字を表示します。
- RIBで使用できない場合、FRRは設定済みのネットワークをアドバタイズしません。

●動的ルーティング(OSPF)
- OSPFは、L2TPトンネルのリモート側ネットワークを再配布しません。

●Eメール
- レガシーメールモードが頻繁にクラッシュします。
- ファームウェアをバージョン19に更新した後、[電子メール] > [一般設定]の下のいくつかの設定をクリックできません。
- スパムメールは、「スパム スキャンに失敗しました」というエラーで通過します。
- スパム対策サービスを開始できません。
- getSmtpQuarantineMailRecordのSQLi。
- Eximによる高いCPU使用率。
- SPXの使用中に添付ファイルが破損する。
- メールログページが読み込み中の状態でスタックします。
- SPXは、指定されていない期間後に動作を停止します。
- 任意のファイル書き込みにより、DoSが作成され、場合によってはRCEベクターが作成されます。
- グローバルSQLエスケープ関数の論理エラーにより、インジェクションが可能になる場合があります。
- MailScanRuleManage.jsに保存された潜在的なXSS
- ファイアウォールルールでSMTPスキャンが有効になっている場合、受信メールは配信されません。
- スマートホスト認証が機能しませんでした。パスワード復号化の失敗に関連しています。
- apxxファイルでのAviraエンジンエラー。
- 返されるヒットが多すぎる場合のSASI検出の問題。
- メールのRCAが「smtp_check_forward_reply: response received without any command」というエラーで受信されませんでした。
- AVスキャンの失敗によるメールループ。
- リリースリンクの設定は検疫ダイジェストに保存できません。
- Awarrensmtpサービスが応答していません。
- pop.ocn.ne.jpドメインの証明書エラーでメールの送受信ができません。

●ファイアウォール
- ファイアウォールルールの作成中にXML APIでエラーが発生したため、バックアップ/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。
- バックアップと復元でアプライアンスへのアクセスが失われました。ローカルACLルールがバックアップと復元で機能しなくなりました。
- 無効な負荷分散NATルールが、無効なNATルールのアラートを引き続き送信します。
- APIControllerを介した認証後の読み取り専用SQLi(CVE-2022-3710)。
- 複数のホストが追加されたときのDNATの問題。
- ファイアウォールルールによる国のブロックが機能していません。
- Netlink:プロセス「ipsetelite」で属性を解析した後に残った153776バイト。
- httperf接続レートテスト中にFP fw_fp_track_connおよびfw_fp_reclaim_connエラーが表示される-(フロー2)。
- サマータイムが正しく反映されていません。
- デバイスのフリーズの問題(0010:queued_spin_lock_slowpath+0x14b/0x170)
- カーネルパニック。カーネルNULLポインター"ip_route_me_harder"を処理できません。
- ファイアウォールルールグループが重複しています。
- 複数のローカルACLルールが構成されている場合、バックアップの復元と移行は失敗します。
- 2ページ目に作成されたゾーンを削除した後、[ゾーン]タブに空白が表示される。
- ファイアウォールが自動的に再起動します。

●ファームウェア管理
- ファイル名にスペースが含まれていると、ファームウェアの更新に失敗します。

●FQDN
- ワイルドカードFQDNホストのIPsetが散発的に作成されない。
- クライアントにVCR以外のDNSサーバーが設定されている場合、サブドメインの学習が機能しません。
- 短いTTL(2～5秒)で解決されるFQDNは、ワイルドカードFQDN ホストで問題を引き起こしています。

●ゲートウェイ管理
- RCA:特定のWANポートのDGD設定を変更できません。

●ホットスポット
- ユーザーポータルのホットスポットバウチャーの場合、[管理]の下にある削除アイコンは直感的ではありません。
- WLANバウチャーが正しく表示されない。
- ユーザーポータルでの認証後の読み取り専用SQLi(CVE-2022-3711)。
- ホットスポットバウチャーの作成に失敗します。
- ホットスポットバウチャーのユーザーポータルでは、並べ替え機能が正しく機能しません。

●インターフェイス管理
- InterfaceHelper.java(objStr)の複数の認証後読み取り専用SQLi脆弱性。
- アプリケーションで見つかったSQLインジェクション。
- LAGインターフェイスを削除できません。

●IPSエンジン
- ATPパターンの更新によるSnortのメモリ使用量の増加。

●IPSルールセット管理
- IPSパターンが更新されません。

●IPS-DAQ
- FirefoxブラウザーでOCSP必須の設定が原因で、Webサイトが機能しません。

●IPS-DAQ-NSE
- 一部のサイトの閲覧時に接続が信頼できない。
- VCRを介してWebサーバーにアクセスできず、SSL/TLSインスペクションエラー「TLS内部エラーが原因でドロップされました」が表示されます。
- do-not-decryptモードでSSL/TLSインスペクションがオンになっていると、大きなファイルをアップロードできません。

●IPsec
- 重複するSAが作成されています。
- BGPサービスが再起動し続け、Amazon VPC接続に影響を与えます。
- NC-84750の問題は、パッチのインストール後も1つのサイトで発生します。
- IPsecルートの送信元IPアドレスが間違っています。
- DDNSを使用する場合、IPsec構成のゲートウェイエントリが異なります。
- XFRMインターフェイスがPPPoEで作成されている場合、ランダムな切断イベントの後にPPPoEが接続されません。
- IPsec VPNフェイルバックが機能していません。
- SMBファイル転送が停止し、IPsecアクセラレーションとポリシーベースのVPNで回復しません。
- メモリ使用量は20～25日間で90%に増加しました。
- VPNトンネル構成を更新すると、Web管理コンソールにエラーが表示されます。
- WWANでxfrmインターフェイスが作成されている場合、ランダムな切断イベントの後にWWANが接続されません。
- ルートの優先順位がVPNに設定され、リモートサブネットがAnyに設定されている場合、システムによって生成されたトラフィックが影響を受けます。
- 絶え間ないIPsecVPNフラッピング。Central SD-WANオーケストレーションを介してプッシュされます。
- 補助デバイスが散発的にIPsecパケットを受信します。
- .scxファイルが無効なため、IPsecリモートアクセスに接続できません。
- IPsecアクセラレーションでのIPsecVPNパスMTU関連の接続の問題。

●L2TP
- アップグレード後、L2TPに接続できません。

●ロギングフレームワーク
- データベースディスクイメージの形式が正しくないことを示すエラーにより、デバイスでのロギングが停止しました。
- オンボックスレポートがオフの場合でも、ログインイベントのPGトリガーエントリが存在する必要があります。
- Central Reporting:Sophos Centralに接続されていない状態でキューの制限に達した場合、mmapケースを開始できませんでした。

●nSXLd
- 「nSXLd:SXLサーバーへの接続中に接続がタイムアウトしました」というエラーでインターネットがダウンする。
- 外部URLデータベースを使用してURLとIPアドレスを分類できません。

●PPPoE
- PPPoEパスワードの問題。

●レポート
- XSSペイロードを持つユーザー名を持つユーザーがいる場合、最終アクセス時刻は生成されません。

●SDWANルーティング
- インポート/エクスポートは、SD-WAN PBRプロファイルの変更を反映しません。
- SD-WANパフォーマンスグラフに格納されたXSS。
- SD-WAN FTPプロキシトラフィックが透過プロキシで機能しない。
- TFTPトラフィックはSD-WANルーティングに従いません。
- VPNゾーンでキャプチャをオフにしても、SD-WANルーティングを使用するルートベースのVPNでは機能しません。

●セキュリティハートビート
- delay-missing-heartbeat-detectionが補助デバイスで同期されていません。

●スプーフィング
- 関連するゾーンでスプーフィング保護が有効になっている場合、ブリッジを通過するトラフィックはIP_Spoofとしてブロックされます。

●SSLVPN
- SSLVPN構成のアップロードによるOSコマンドインジェクション(CVE-2022-3226)。
- SSLVPNサイト間サーバー構成をダウンロードできません。
- AndroidおよびiOSユーザーは、SSLVPN ovpnファイルをインポートできません。
- SSLVPNサービスがビジー状態のままになっています。サイト間およびリモートアクセスSSLVPNが影響を受けます。
- トンネルが稼働しているにもかかわらず、トラフィックがサイト間SSLVPNトンネルを通過していません。
- SSLVPNグローバル設定の変更後、SecurityHeartbeat_over_VPNオブジェクトがSSLVPNポリシーから削除されました。
- CVE:2022-0547 openvpn遅延認証の脆弱性。
- サイト間およびリモートアクセスSSLVPNが機能しない。
- ダッシュボードにはリモートユーザーの詳細が反映されません。
- /conf/certificate/openvpnディレクトリがありません。
- 19.0.MR1にアップグレードした後、リモートアクセスSSLVPNが機能しません。

●UIフレームワーク
- 認証後のコードインジェクション(CVE-2022-3696)。

●Up2Dateクライアント
- ファームウェアのダウングレード後のSASIパターンの表面的な問題。

●WAF
- WAFルールに選択した後、WAF保護ポリシーを変更または更新できません。
- 例外を含むアプリケーション攻撃グループのCRSルールをスキップできません。
- WAFルールが機能していません。
- ModSecurityとOWASP CRSを最新バージョンにアップグレードします。
- ファイアウォールルールが無効になっている場合、仮想ホストは削除されません。
- 暗号化されたWAFシークレットのAPI JSONフィールドを更新します。
- IPホスト経由でXSSがWAF例外に格納されました。

- サブジェクト代替がドメインの一部ではないという警告。

●ウェブ
- カスタムカテゴリ名は、URLカテゴリルックアップにXSSを格納しました。
- ゼロデイ保護レポートに、ライセンスの警告が正しく表示されません。
- 新しい証明書を生成するのではなく、certcache内の期限切れの証明書が使用されます。
- ドイツ語でサインインしている場合、Webプロキシ設定の変更を保存できません。
- ユーザー通知設定でユーザー定義のロゴをアップロードすると、エラーが発生します。

●WebInSnort
- libnsg_tcphold_preprocでのIPSセグメンテーション違反。
- 8080上の内部サーバーへのHTTPSトラフィックは、ips tcpholdによってドロップされます。

●ワイヤレス
- LocalWiFi mac80211の脆弱性。
- Wi-Fiコントローラーでの隣接コードインジェクション(CVE-2022-3713)。
- ブリッジインターフェイスのゲストAPのMacエージングタイムが正しくありません。
- 高速移行がオンになっていると、レガシーAPローミングキーの復号化が失敗します。
- 時間ベースのSSIDが設定されている場合、再起動後にVCROSが不良ステータスになります。
- アップデート後、セパレートゾーンSSIDのageging_timeパラメータは0にリセットされます。

●XGS-BSP
- NPUの障害によるフェイルセーフの問題。
- ランダムSFP+ポートフラップ。