既知の問題

便宜上、このリリースノートには、このバージョンの既知のバグが記載されています。

（注） このリストは1回自動生成され、その後は更新されません。バグがシステムでどのように分類または更新されたかとその時期によっては、リリースノートに記載されない場合があります。Cisco Bug Search Tool を「信頼できる情報源」と考えてください。

アップグレードでバージョンがスキップされる場合は、スキップするメジャーバージョンの既知の問題も参照してください。「Cisco Firepower リリース ノート」を参照してください。

既知の問題の検索

サポート契約がある場合は、Cisco Bug Search Tool を使用して Firepower 製品の最新のオープンバグリストを取得することができます。 検索では、特定の Firepower プラットフォームとバージョンに影響するバグに絞り込むことができます。バグ ID ごとに検索したり、特定のキーワードを検索したりすることもできます。

これらの一般的なクエリには、Version6.2.3を実行している Firepower 製品の未解決のバグが表示されます。

- Firepower Management Center
- Firepower Management Center Virtual
- Firepower Threat Defense
- Firepower Threat Defense Virtual
- ASA with FirePOWER サービス
- NGIPSv

バージョン 6.2.3 の既知の問題

表 *1* : バージョン *6.2.3* の既知の問題

不具合 ID	タイトル
CSCvf16001	SF Cli：「inside」または「outside」インターフェイス キャプチャではすべてのオプションが提供されない
CSCvh73096	Firepower Management Center は、ISE 2.2+ を使用したログインで userPrincipalName 属性をサポートしない
CSCvh89068	Firepower Management Center Perl のコア
CSCvh95960	capture コマンドで **match** キーワードを使用すると、キャプチャで IPv6 トラフィックが無視される
CSCvi07656	ハードウェア モードの TLS インスペクションが過負荷になると、少数の TLS 接続が失敗する可能性がある
CSCvi10758	ソフトウェア モードの SSL インスペクションを使用すると、いくつかの TLS 接続が適切なタイミングで終了しない
CSCvi16024	サーバの IP アドレスが変更されるとセッションが再開する場合の SSL エラー（HW モード）
CSCvi18123	2100 で CLISH CLI からの Firepower Threat Defense **show tech-support** コマンドの出力が破損する
CSCvi19862	SSL インスペクションを有効にすると、TLS トラフィックのスループットにより、後続のハイ アベイラビリティ フェールオーバーがドロップされる可能性がある
CSCvi35176	展開の失敗：Snort の再起動に失敗する：**APPLY_APP_CONFIG_APPLICATION_FAILURE** SignalAppConfigFailed
CSCvi35588	「**Snort failed to restart** PDTS Handle was NULL」が原因で展開が失敗する
CSCvi42539	SSLv2 がサポートされているが、より高いバージョンがネゴシエートされる場合、復号化された接続が失敗する
CSCvi47264	TAXII フィードを並行して使用すると、一部のインジケータが保留状態のままになる場合がある
CSCvi49538	2100で Firepower デバイス管理が失敗する（6.2.3 ～ 51（PortChannel））
CSCvi50731	以前に ISE で使用された証明書オブジェクトがあり、削除された場合でも、証明書オブジェクトを削除できない

不具合 ID	タイトル
CSCvi61411	ルーティングされた Threat Defense では透過的な設定が可能であるが、KVM でのみでトラフィックが失敗する（6.2.3 ～ 66）
CSCvi62982	ESXi Firstboot config の Firepower Threat Defense Virtual では、ホスト名が FQHN と適切に同期されない
CSCvi63157	Firepower 2110 が接続をドロップする
CSCvi63864	ハードウェア モードの SSL インスペクションとマルウェア防御で、安全なファイル転送が失敗することがある
CSCvi66189	ライセンスのためにサテライト サーバを使用している Firepower Management Center で CNP が有効にされている
CSCvi70680	異なる AD の同じグループがダウンロードされない
CSCvv14442	将来のタイムスタンプを持つファイル/ディレクトリが含まれている場合、FMC バックアップの復元が失敗する