H3Cアクセスコントローラ
WIPSエラーメッセージ

エラーレベルの見方

エラー名	状況説明	重大度レベル
緊急(emergency)	システムが動作していません	重大度= 0
アラート(alert)	推奨アクションはすぐに実行する必要があります	重大度= 1
クリティカル(critical)	危機的な状態	重大度= 2
エラー(error)	エラー状態	重大度= 3
警告(warning)	警告条件	重大度= 4
通知(notification)	正常だが重大な状態	重大度= 5
情報(informational)	情報メッセージ	重大度= 6
デバッグ(debugging)	デバッグレベルのメッセージ	重大度= 7

WIPSメッセージ

WIPS_APFLOOD

メッセージ文	-VSD=[STRING]; AP flood detected.
変数フィールド	$1: VSD name.
重大度レベル	5
例	WIPS/5/APFLOOD: -VSD=home; AP flood detected.
説明	指定されたVSDで検出されたAPの数がしきい値に達しました。
推奨される対処	デバイスが攻撃を受けたかどうかを確認します。

WIPS_AP_CHANNEL_CHANGE

メッセージ文	-VSD=[STRING]-SrcMAC=[MAC]; Channel change detected.
変数フィールド	$1: VSD name. $2: MAC address of the AP.
重大度レベル	5
例	WIPS/5/AP_CHANNEL_CHANGE: -VSD=home-SrcMAC=1122-3344-5566; Channel change detected.
説明	指定されたAPのチャネルが変更されました。
推奨される対処	チャネルの変更が有効かどうかを確認します。

WIPS_ASSOCIATEOVERFLOW

メッセージ文	-VSD=[STRING]-SrcMAC=[MAC]; Association/Reassociation DoS attack detected.
変数フィールド	$1: VSD name. $2: MAC address of the AP.
重大度レベル	5
例	WIPS/5/ASSOCIATEOVERFLOW: -VSD=home-SrcMAC=1122-3344-5566; Association/Reassociation DoS attack detected.
説明	指定されたAPは、ステータスコード17の関連付け応答を送信しました。
推奨される対処	APが攻撃を受けたかどうかを判断します。

WIPS_DOS

メッセージ文	-VSD=[STRING]; [STRING] rate attack detected.
変数フィールド	$1: VSD name. $2: Device type: AP or client.
重大度レベル	5
例	WIPS/5/WIPS_DOS: -VSD=home; AP rate attack detected.
説明	指定された間隔内に学習されたデバイスエントリの数がしきい値に達しました。
推奨される対処	デバイスが攻撃を受けているかどうかを確認します。

WIPS_FLOOD

メッセージ文	-VSD=[STRING]-SrcMAC=[MAC]; [STRING] flood detected.
変数フィールド	$1: VSD name. $2: Attacker's MAC address. $3: Flood attack type. Options include the following: • Association request • Authentication • Disassociation • Reassociation request • Deauthentication • Null data • Beacon • Probe request • BlockAck • CTS • RTS • EAPOL start
重大度レベル	5
例	WIPS/5/WIPS_FLOOD: -VSD=home-SrcMAC=1122-3344-5566; Association request flood detected.
説明	指定された間隔内に検出された特定のタイプのパケットの数がしきい値に達しました。
推奨される対処	パケット送信者が許可されたデバイスであるかどうかを確認します。

WIPS_HONEYPOT

メッセージ文	-VSD=[STRING]-SrcMAC=[MAC]; Honeypot AP detected.
変数フィールド	$1: VSD name. $2: MAC address of the AP.
重大度レベル	5
例	WIPS/5/HONEYPOT: -VSD=home-SrcMAC=1122-3344-5566; Honeypot AP detected.
説明	指定されたAPがハニーポットAPとして検出されました。
推奨される対処	デバイスが攻撃を受けたかどうかを確認します。

WIPS_HTGREENMODE

メッセージ文	-VSD=[STRING]-SrcMAC=[MAC]; HT-Greenfield AP detected.
変数フィールド	$1: VSD name. $2: MAC address of the AP.
重大度レベル	5
例	WIPS/5/HTGREENMODE: -VSD=home-SrcMAC=1122-3344-5566; HT-Greenfield AP detected.
説明	指定されたAPはHTグリーンフィールドAPとして検出されました。.
推奨される対処	デバイスが攻撃を受けたかどうかを確認します。

WIPS_MALF

メッセージ文	-VSD=[STRING]-SrcMAC=[MAC]; Error detected: [STRING].
変数フィールド	$1: VSD name. $2: Sender's MAC address. $3: Malformed packet type. Options include the following: • **invalid ie length**—Invalid IE length. • **duplicated ie**—Duplicate IE. • **redundant ie**—Redundant IE. • **invalid pkt length**—Invalid packet length. • **illegal ibss ess**—Abnormal IBSS and ESS setting. • **invalid source addr**—Invalid source MAC address. • **overflow eapol key**—Oversized EAPOL key. • **malf auth**—Malformed authentication request frame. • **malf assoc req**—Malformed association request frame. • **malf ht ie**—Malformed HT IE. • **large duration**—Oversized duration. • **null probe resp**—Malformed probe response frame. • **invalid deauth code**—Invalid deauthentication code. • **invalid disassoc code**—Invalid disassociation code. • **over flow ssid**—Oversized SSID. • **fata jack**—FATA-Jack.
重大度レベル	5
例	WIPS/5/WIPS_MALF: -VSD=home-SrcMAC=1122-3344-5566; Error detected: fata jack.
説明	不正な形式のパケットが検出されました。
推奨される対処	パケット送信者が許可されたデバイスであるかどうかを確認します。

WIPS_MAN_IN_MIDDLE

メッセージ文	-VSD=[STRING]-SrcMAC=[MAC]; Man-in-the-middle attack detected.
変数フィールド	$1: VSD name. $2: MAC address of the client.
重大度レベル	5
例	WIPS/5/MAN_IN_MIDDLE: -VSD=home-SrcMAC=1122-3344-5566; Man-in-the-middle attack detected.
説明	指定されたクライアントが中間者攻撃を受けました.
推奨される対処	クライアントが中間者攻撃を受けたかどうかを判断します。

WIPS_Rogue_AP

メッセージ文	-VSD=[STRING]-SrcMAC=[MAC]; Rogue AP detected by radio 1 of sensor [STRING] on channel 149 (RSSI=84).
変数フィールド	$1: VSD name. $2: MAC address of the rogue AP.
重大度レベル	5
例	WIPS/5/WIPS_ROGUE: -VSD=home-SrcMAC=1122-3344-5566; Rogue AP detected by radio 1 of sensor ap1 on channel 149 (RSSI=84).
説明	不正なAPが検出されました。
推奨される対処	WIPSが不正APに対する対策を講じられるようにします。

WIPS_SPOOF

メッセージ文	-VSD=[STRING]-SrcMAC=[MAC]; [STRING] detected.
変数フィールド	$1: VSD name. $2: MAC address of the device being spoofed. $3: Spoofing attack type. Options include the following: • **AP spoofing AP**—A fake AP spoofs an authorized AP. • **AP spoofing client**—A fake AP spoofs an authorized client. • **AP spoofing ad-hoc**—A fake AP spoofs an Ad hoc device. • **Ad-hoc spoofing AP**—An Ad hoc device spoofs an authorized AP. • **Client spoofing AP**—A client spoofs an authorized AP.
重大度レベル	5
例	WIPS/5/WIPS_SPOOF: -VSD=home-SrcMAC=1122-3344-5566; AP spoofing AP detected.
説明	なりすまし攻撃が検出されました。
推奨される対処	パケット送信者が許可されたデバイスであるかどうかを確認します。

WIPS_Unauth_Client

メッセージ文	-VSD=[STRING]-SrcMAC=[MAC];Unauthorized client detected by radio 1 of sensor [STRING] on channel 149 (RSSI=84).
変数フィールド	$1: VSD name. $2: MAC address of the unauthorized client.
重大度レベル	5
例	WIPS/5/WIPS_UNAUTH: -VSD=home-SrcMAC=1122-3344-5566; Unauthorized client detected by radio 1 of sensor ap1 on channel 149 (RSSI=84).
説明	許可されていないクライアントが検出されました.
推奨される対処	許可されていないクライアントが存在するかどうかを確認します。

WIPS_WEAKIV

メッセージ文	-VSD=[STRING]-SrcMAC=[MAC]; Weak IV detected.
変数フィールド	$1: VSD name. $2: Sender's MAC address.
重大度レベル	5
例	WIPS/5/WIPS_WEAKIV: -VSD=home-SrcMAC=1122-3344-5566; Weak IV detected.
説明	弱いIVが検出されました。
推奨される対処	より安全な暗号化方式を使用して、パケットを暗号化します。

WIPS_WIRELESSBRIDGE

メッセージ文	-VSD=[STRING]-AP1=[MAC]-AP2=[MAC]]; Wireless bridge detected.
変数フィールド	$1: VSD name. $2: MAC address of AP 1. $3: MAC address of AP 2.
重大度レベル	5
例	WIPS/5/WIRELESSBRIDGE: -VSD=home-AP1=1122-3344-5566-AP2=7788-9966-5544; Wireless bridge detected.
説明	指定されたAPはワイヤレスブリッジをセットアップします。
推奨される対処	ワイヤレスブリッジが有効かどうかを確認します。