Zimperium zConsole

Threat Reference Guide

Document ID: 924-10 (Release 4.38+)

March 2022

Table of Contents

Preface

This guide details the list of threats in the zConsole. The threats are managed on the **Policy** page of zConsole. This document includes information on which threats are supported on Android and iOS. In addition, the guide details the threats supported in the zIPS application and in the zDefend SDK framework.

This document assumes an overall knowledge of Zimperium terms. For more overview information see the "*zConsole Configuration Guide*."

Audience

The intended audience for this guide is zConsole system administrators and zDefend SDK developers. The zConsole application provides threat protection to mobile devices. The system administrator sets policies for threats, and also monitors and manages threats detected. Developers often need a list of threats to integrate with an MDM or to build a mobile application using the zDefend SDK framework.

Related Documentation

Additional Zimperium documents are located on the Customer Support Portal at the website: http://support.zimperium.com

Overview

Mobile devices are found everywhere today. They represent an opportunity for malicious actors who are looking to find new ways to gain access to corporate environments. Although corporate environments may have protection from viruses and malicious code on servers, desktops, and laptops, mobile devices are increasingly the new frontier that is being colonized by hackers.

This document provides information on the threat classifications. These threat classifications are presented in the zConsole **Policy** page where system administrators can set severity levels and the desired actions to notify for threats and mitigate actions to the threats.

Threat Policy

The Threat Policy defines the zIPS actions when detecting an event. This is managed on the **Policy** page in the zConsole. The options include:

- Enable or disable detection of a specific threat classification.
- Alert the user or not.
- Define the text of the alert.
- Define the protection actions to take, such as local at the device or MDM related.
- Define if an email, SMS text, or both are to be sent to the logged-in administrator.

When you finish modifying these options, the policies are deployed to the logged-in zIPS devices. See the "*zConsole Configuration Guide*" for more information on the v4 zConsole functionality. See the online documentation for the zDefend console information.

> ***Note**: With the zConsole Release 4.30, new threats can be added dynamically to the list of threats displayed on the **Policy** page. By default, new threats are added as disabled for existing policies and enabled for new policies.*

Threats

This section contains the list of threats along with information that describes more information about them.

Threat Information

The threat table lists the threats that are displayed on the zConsole **Policy** page. The columns include:

- **Threat Name**: This is the name of the threat. The table is in alphabetical order by threat name.
- **Threat Description**: This is a description of the threat and has these values:
    - Descriptive text of the threat.
    - Threat mitigation whether it is automatic or manual. See "About Manual and Automatic Mitigation" for more information.
    - The vector for the threat, where the list of vector values is Device, App, and Network.
    - The threat tag value that some customers use in integrations.
    - The MITRE tactics, if applicable. The MITRE tactic information is available in the zConsole when you select the information icon.
    - A threat active date for some threats is the date when the threat was added dynamically to zConsole.

      See the "*zConsole Configuration Guide*" for more information about vectors, mitigation, and MITRE tactics.

- **Risk or Threat**: This indicates if the threat is a potential risk or an actual threat.
- **Severity Default**: This is the default severity for the threat, for example, Low, Normal, Elevated, or Critical.
- **Android OS**: This column indicates if the threat is supported on an Android device.
- **Apple OS**: This column indicates if the threat is supported on an iOS device.
- **Chrome OS**: This column indicates if the threat is supported on a Chrome OS device.
- **zIPS**: This column indicates if the threat is supported in the zIPS application. Some entries have the zIPS release number in parentheses, indicating in what release it is supported.
- **zDefend SDK**: This column indicates if the threat can be returned by the zDefend SDK framework. Some entries have the zDefend SDK release number in parentheses, indicating in what release it is supported.
- **Threat Identifiers**: This column has two internal identifiers values for a threat. The text identifier value is followed by a comma, and then the numerical identifier value. These are used by zDefend SDK users in building their own apps.

  ***Note**: The items marked with the letter "a" with the notation [a] indicate that Hotspot Helper is required for iOS functionality support. Other threats have letters in square brackets for additional notes with the legend at the end of the threat list table. See "Threat List Legend" for the legend list.*

About Manual and Automatic Mitigation

Mitigating a threat is making the threat less of a risk or removing the risk altogether. Each threat indicates if it has automatic or manual mitigation. Automatic mitigation means that changes to the device or other risk factors can change, and the threat can be automatically mitigated through zConsole or zIPS software. The status of the threat then changes from a Pending state to a Fixed state.

Manual mitigation means that an administrator must mark the threat as fixed or approved. See the "*zConsole Configuration Guide*" for more information on these actions.

For threats marked as automatic mitigation, if the device:

- Is reset to factory settings or reimaged
- Has the zIPS app removed from the device

then threats can be left in the Pending state in the threat log and need manual mitigation.

About the Dynamic Nature of Threats

This document captures the threat information in one location for ease of reference. However, after zConsole Release 4.30 and zConsole Release 5.11, threat data is dynamically managed, instead of static for each release. Therefore, some of the values like severity default, or even the list of threats, can change before a release of this document can capture the delta.

Threat List Legend

This legend describes the indicators in square brackets that give additional information to the threats.

[a] = Indicates that for iOS support, Hotspot Helper is required.
[b] = Indicates that for iOS threat support, an MDM server to sync with the zConsole is required.
[c] = Indicates that the server detects the threat and sends a notification (email) without a device alert display within the application.
[d] = Indicates the value is really mitigation of a previous MITM-ARP threat.
[e] = MITM – ARP is supported on iOS 10 only. For iOS 11 and above, the MITM attacks are detected under the threat name MITM.
[f] = Indicates that the threat is a composite threat. See the "zConsole Configuration Guide" for definitions of composite and singular threats.
[g] = Indicates that a particular type of Rogue Access Point threat called KARMA is only supported by Android OS 9 and earlier.
[h] = Indicates that the zDefend SDK can return this threat, but the threat only applies when interfacing with the v4 zConsole.
[i] = The mitigation can be either manual or automatic depending on the set of attacks that occurred to trigger this composite threat.

Threat List

Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
Abnormal Process Activity	Detected abnormal activity. Your device is being monitored for any attacks. **Mitigation**: Manual **Vector**: Device **Tag**:host.process.activity **MITRE Tactics**: Execution, Persistence, Impact	Risk	Elevated	Yes (OS<=6 & Knox >= 3.4+)	Jailbroken Devices Only	Yes	Yes	Yes	ABNORMAL_PROCESS_ACTIVITY, 10
Always-on VPN App Set	An app has been configured as an always-on VPN on this device. The app may monitor all device communications with the Internet. **Mitigation**: Automatic **Vector**: Device **Tag**:host.always_on_vpn_app **MITRE Tactics:** Collection, Exfiltration, Network Effects	Risk	Elevated	Yes	---	Yes	Yes (4.8)	Yes (4.8)	ALWAYS_ON_VPN_APP_SET, 87
Android Debug Bridge (ADB) Apps Not Verified	Apps installed via ADB are not required to be verified. This may allow malicious apps to be installed on the device. **Mitigation**: Automatic **Vector**: Network **Tag**:host.adb_apps_not_verified **MITRE Tactics:** Initial Access, Privilege Escalation, Persistence, Credential Access, Lateral Movement, Collection, Exfiltration	Risk	Elevated	Yes	---	Yes	Yes (4.8)	Yes (4.8)	ANDROID_DEBUG_BRIDGE_APPS_NOT_VERIFIED, 85

Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
Android Device - Compatibility not tested by Google	The profile of the Android device does not match the profile of any devices that have passed Google's Android compatibility testing. **Mitigation**: Automatic **Vector**: Device **Tag**:host.SafetyNetAttestation.ctsProfileMatch-false **MITRE Tactics:** Initial Access, Impact	Risk	Low	Yes	---	---	Yes (4.4)	Yes (4.4)	ANDROID_COMPATIBILITY_TESTING, 70
Android Device - Possible Tampering	Possible tampering may have occurred with the Android device. **Mitigation**: Automatic **Vector**: Device **Tag**:host.SafetyNetAttestation.basicintegrity-false **MITRE Tactics:** Execution, Persistence, Privilege Escalation, Impact	Threat	Critical	Yes	---	Yes	Yes (4.4)	Yes (4.4)	ANDROID_BASIC_INTEGRITY, 71
App Debug Enabled	An app with debug enabled can pose a risk and allow an attacker to control and manipulate the underlying app functions. **Mitigation**: Automatic **Vector**: Device **Tag**:host.app_attached_to_debugger **MITRE Tactics:** n/a	Risk	Elevated	Yes	---	---	Yes (4.16)	Yes (4.16)	DEBUG_ENABLED_APK, 103
App Pending Activation	App activation for the Mobile Threat Defense (MTD) application is not complete. Notification email: [c] **Mitigation**: Automatic **Vector**: Device **Tag**:host.device_pending_activation **MITRE Tactics:** n/a	Risk	Low	Yes	Yes	Yes	Yes	Yes	DEVICE_PENDING_ACTIVATION, 200

Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
App Running on Emulator	An app running on an emulator can pose a risk and allow an attacker to control and manipulate the underlying operating environment. **Mitigation**: Automatic **Vector**: Device **Tag**:host.app_running_on_emulator **MITRE Tactics:** n/a	Threat	Critical	Yes	---	---	---	Yes (4.16)	DEVICE_EMULATOR, 104
App Tampering	Existing app libraries may have been modified, or a foreign library may have been injected into the app. **Mitigation**: Automatic **Vector**: Device **Tag**:host.app_tampering **MITRE Tactics:** Execution, Persistence, Privilege Escalation, Defense Evasion	Threat	Critical	Yes	Yes	Yes	Yes (4.4)	Yes (4.4)	APP_TAMPERING, 75
ARP Scan	A reconnaissance scan using the ARP protocol is often an indicator of a malicious attacker searching for a device vulnerable to a network attack, such as MITM. **Mitigation**: Automatic **Vector**: Network **Tag**:network.scan.arp **MITRE Tactics:** Network Effects, Discovery, Collection	Risk	Normal	Yes (OS<=9)	Yes (OS<=9)	---	Yes	Yes	ARP_SCAN,3

Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
BlueBorne Vulnerability	The device is vulnerable to a BlueBorne attack, which leverages Bluetooth connections to penetrate and take control of targeted devices. To avoid any risk from BlueBorne, the user needs to permanently turn off Bluetooth until an update is available from your device manufacturer or wireless carrier. For those users that still require the use of Bluetooth, it is recommended that Bluetooth is turned off until it is needed and only in a trusted and secure area. **Mitigation**: Automatic **Vector**: Device **Tag**:host.blueborne_vulnerability **MITRE Tactics:** Initial Access, Remote Service Effects	Risk	Elevated	Yes	--- (Yes for OS<= 9.3.5)	Yes	Yes	Yes	BLUEBORNE_VULNERABLE, 69
Captive Portal	Captive portal networks route traffic through a single proxy (portal), potentially opening up the traffic to monitoring. **Mitigation**: Automatic **Vector**: Network **Tag**:network.captive_portal **MITRE Tactics:** Network Effects, Initial Access	Risk	Normal	Yes	Yes [a]	Yes	Yes	Yes [a]	CAPTIVE_PORTAL, 67

Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
Compromised Network	A pattern of threats occurred that indicates the device is connected to a compromised network. Sensitive data on the device may be intercepted and could be monitored and modified by an unauthorized party. Type is composite. [f] **Mitigation**: Automatic **Vector**: Network **Tag**:pattern.compromised_network **MITRE Tactics:** Initial Access, Collection, Exfiltration, Network Effects	Threat	Critical	Yes	Yes	Yes	Yes (4.17)	Yes (4.17)	COMPROMISED_NETWORK, 125
Daemon Anomaly	A daemon anomaly indicates abnormal system process activities that can indicate that the device has been exploited. **Mitigation**: Automatic **Vector**: Device **Tag**:host.daemon_anomaly **MITRE Tactics:** Execution, Persistence, Privilege Escalation	Risk	Low	Yes (OS<=6 & Knox >= 3.4+)	---	---	Yes	Yes	DAEMON_ANOMALY, 43
Danger Zone Connected	The device connected to a Wi-Fi network where malicious attacks have been observed. **Mitigation**: Automatic **Vector**: Network **Tag**:network.danger_zone_connected **MITRE Tactics:** Initial Access, Network Effects	Threat	Low	Yes	Yes	Yes	Yes (4.4)	Yes (4.7) [h]	DANGERZONE_CONNECTED, 79

Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
Danger Zone Nearby	The device is near a Wi-Fi network where malicious attacks have been observed. **Mitigation**: Automatic **Vector**: Network **Tag**:network.danger_zone_nearby **MITRE Tactics:** Initial Access, Network Effects	Risk	Normal	Yes	Yes [a]	Yes	Yes (4.4)	Yes (4.7) [h]	DANGERZONE_NEARBY, 80
Detection Inactive	MTD detection is inactive. **Mitigation**: Automatic **Vector**: Device **Tag**:host.detection_inactive **MITRE Tactics:** n/a **Threat Active Date**: February 2022	Risk	Elevated	Yes	Yes	Yes	Yes (4.20.4)	---	DETECTION_INACTIVE, 1007
Detection Pending Activation	MTD detection is pending activation. **Mitigation**: Automatic **Vector**: Device **Tag**:host.detection_pending_activation **MITRE Tactics:** n/a **Threat Active Date**: February 2022	Risk	Low	Yes	Yes	Yes	Yes (4.20.4)	---	DETECTION_PENDING_ACTIVATION, 1006
Developer Options	Developer Options is an advanced configuration option intended for development purposes only. When enabled, the user has the option to change advanced settings, compromising the integrity of the device settings. **Mitigation**: Automatic **Vector**: Device **Tag**:host.developer_options **MITRE Tactics:** Impact	Risk	Low	Yes	---	Yes	Yes	Yes	DEVELOPER_OPTIONS_ON, 47

Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
Device Compromised via iOS Malicious Profile	The device was compromised by a sophisticated kill chain attack that started with a malicious iOS profile and ended leaving the device compromised. Type is composite. [f] **Mitigation**: Manual **Vector**: Device **Tag**:pattern.device_compromised_via_ios_malicious_profile **MITRE Tactics:** Initial Access, Execution, Persistence, Privilege Escalation, Credential Access, Collection, Exfiltration, Impact	Threat	Critical	---	Yes	---	Yes (4.17)	Yes (4.17)	DEVICE_COMPROMISED_VIA_IOS_MALICIOUS_PROFILE, 124
Device Compromised via Malicious App	The device was compromised by a sophisticated kill chain attack that started with a malicious app and ended leaving the device compromised. Type is composite. [f] **Mitigation**: Manual or Automatic [i] **Vector**: Device **Tag**:pattern.device_compromised_via_malicious_app **MITRE Tactics:** Initial Access, Execution, Persistence, Privilege Escalation, Credential Access, Collection, Exfiltration, Impact	Threat	Critical	Yes	Yes	Yes	Yes (4.17)	Yes (4.17)	DEVICE_COMPROMISED_VIA_MALICIOUS_APP, 122

Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
Device Compromised via Network-Based Effects	The device was compromised by a sophisticated kill chain attack that started at the network and ended leaving the device compromised. Type is composite. [f] **Mitigation**: Manual **Vector**: Network **Tag**:pattern.device_compromised_via_network_based_attacks **MITRE Tactics:** Initial Access, Execution, Persistence, Privilege Escalation, Credential Access, Collection, Exfiltration, Impact, Network Effects	Threat	Critical	Yes	Yes	Yes	Yes (4.17)	Yes (4.17)	DEVICE_COMPROMISED_VIA_NETWORK_BASED_ATTACKS, 121
Device Compromised via Phishing Attack	The device was compromised by a sophisticated kill chain attack that started with a phishing threat and ended leaving the device compromised. Type is composite. [f] **Mitigation**: Manual **Vector**: Network **Tag**:pattern.device_compromised_via_phishing_attack **MITRE Tactics:** Initial Access, Execution, Persistence, Privilege Escalation, Credential Access, Impact, Network Effects	Threat	Critical	Yes	Yes	Yes	Yes (4.17)	Yes (4.17)	DEVICE_COMPROMISED_VIA_PHISHING_ATTACK, 123

Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
Device Encryption	Encryption is not set up on the device and is needed to protect the device's content. **Mitigation**: Automatic **Vector**: Device **Tag**:host.encryption **MITRE Tactics:** Impact	Risk	Elevated	Yes	---	n/a	Yes	Yes	ENCRYPTION_NOT_ENABLED, 49
Device Jailbroken/Rooted	Jailbreaking and rooting are the processes of gaining unauthorized access or elevated privileges on a system. Jailbreaking and rooting can potentially open security holes that may not have been apparent or undermine the device's built-in security measures. **Mitigation**: Automatic **Vector**: Device **Tag**:host.jailbroken **MITRE Tactics:** Execution, Persistence, Privilege Escalation	Threat	Critical	Yes	Yes	Yes	Yes	Yes	DEVICE_ROOTED, 39
Device Pin	The device is not set up to use a PIN code or password to control access to the device. **Mitigation**: Automatic **Vector**: Device **Tag**:host.pin **MITRE Tactics:** Impact	Risk	Elevated	Yes	Yes	---	Yes	Yes	PASSCODE_NOT_ENABLED, 50

Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
DNS Change	The DNS configuration changed on the mobile device. If the DNS change happened within your own network to an unknown DNS server, then it is likely a MITM attempt. **Mitigation**: Automatic **Vector**: Device **Tag**:host.config.dns **MITRE Tactics:** Initial Access, Network Effects	Risk	Normal	Yes	---	Yes	Yes	Yes	DNS_CHANGE, 17
Elevation of Privileges (EOP)	A malicious process that results in the elevation of privileges on the mobile device allows an attacker to take full control of the device. **Mitigation**: Manual **Vector**: Device **Tag**:host.process.eop **MITRE Tactics:** Execution, Persistence, Privilege Escalation	Threat	Elevated	Yes (OS<=6 & Knox >= 3.4+)	Yes	---	Yes	Yes	RUNNING_AS_ROOT, 12
File System Changed	A file system change occurred. Modifications made to files in the file system may sometimes lead to a malicious event. **Mitigation**: Automatic **Vector**: Device **Tag**:host.process.filesystemchange **MITRE Tactics:** Persistence, Impact	Threat	Elevated	Yes	Yes	Yes	Yes	Yes	FILES_SYSTEM_CHANGED, 23

Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
Gateway Change	Gateway configuration changes on the mobile device can be indicative of sending traffic to a non-intended destination. **Mitigation**: Automatic **Vector**: Network **Tag**:host.config.gateway **MITRE Tactics:** Initial Access, Network Effects	Risk	Normal	Yes	---	---	Yes	Yes	GATEWAY_CHANGE, 16
Google Play Protect Disabled	Google Play Protect has been disabled on this device. Google Play Protect helps protect the device from malicious apps and needs to be re-enabled. **Mitigation**: Automatic **Vector**: Device **Tag**:host.config.google_play_protect_disabled **MITRE Tactics:** Initial Access, Impact	Risk	Elevated	Yes	---	Yes	Yes (4.5)	Yes (4.5)	GOOGLE_PLAY_PROTECT_DISABLED, 84
High Risk Browser Extension	A Chrome extension is detected that has one or more privacy and/or security concerns that may put your personal and confidential information at risk. **Mitigation**: Automatic **Vector**: App **Tag**:chromeos.extension.high_risk **MITRE Tactics:** n/a **Threat Active Date**: December 2021	Risk	Elevated	—	—	Yes	—	Yes	HIGH_RISK_BROWSER_EXTENSION, 1004

Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
Inactive App	A certain amount of time has passed and the app has not communicated with the server. Notification email: [c] **Mitigation**: Automatic **Vector**: Device **Tag**:app.dormant **MITRE Tactics:** n/a	Risk	Elevated	Yes	Yes	Yes	Yes	---	INACTIVE_APP, 100
Internal Network Access	An app was detected connecting to private or internal servers. It is uncommon for public applications to connect to internal servers. Public applications connecting to internal servers is considered suspicious behavior and needs investigation immediately for the possible threat of malware installed on the device and the risk of data leakage. **Mitigation**: Automatic **Vector**: Network **Tag**:network.internal_network_access **MITRE Tactics:** Discovery, Lateral Movement, Collection	Risk	Low	Yes (OS<=9 & Knox >= 3.4+)	---	---	Yes	Yes	INTERNAL_NETWORK_ACCESS, 48

Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
IP Scan	A reconnaissance scan using the IP protocol is often an indicator of a malicious attacker searching for a device vulnerable to a network attack, such as MITM. **Mitigation**: Automatic **Vector**: Network **Tag**:network.scan.ip **MITRE Tactics:** Initial Access, Discovery, Collection, Network Effects	Risk	Normal	Yes OS<=9)	Yes (OS<=9)	---	Yes	Yes	IP_SCAN, 2
MITM	A man-in-the-middle attack occurred where a malicious attacker can hijack traffic, steal credentials, and deliver malware to the device. **Mitigation**: Automatic **Vector**: Device **Tag**:network.mitm **MITRE Tactics:** Collection, Exfiltration, Network Effects	Threat	Elevated	Yes	Yes	Yes	Yes	Yes	TRACEROUTE_MITM, 68
MITM - ARP	Man-in-the-Middle attack using ARP table poisoning where a malicious attacker can hijack traffic and steal credentials or deliver malware to the device. **Mitigation**: Automatic **Vector**: Network **Tag**:network.mitm.arp **MITRE Tactics:** Collection, Exfiltration, Network Effects	Threat	Elevated	Yes	Yes (OS<=10) [e]	---	Yes	Yes	ARP_MITM, 4

Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
MITM - Fake SSL Certificate	A man-in-the-middle attack using a fake certificate occurred, and this is when a malicious attacker can hijack traffic, steal credentials, and deliver malware to the device. **Mitigation**: Automatic **Vector**: Network **Tag**:network.mitm.ssl_certificate **MITRE Tactics:** Collection, Exfiltration, Network Effects	Threat	Elevated	Yes	Yes	Yes	Yes	Yes	SSL_MITM, 35
MITM - ICMP Redirect	A man-in-the-middle attack using ICMP protocol is when a malicious attacker can hijack traffic, steal credentials, and deliver malware to the device. **Mitigation**: Automatic **Vector**: Network **Tag**:network.mitm.icmp **MITRE Tactics:** Collection, Exfiltration, Network Effects	Threat	Elevated	Yes (OS<=9)	---	---	Yes	Yes	ICMP_REDIR_MITM, 11
MITM - SSL Strip	A man-in-the-middle attack using SSL stripping allows a malicious attacker to change HTTPS traffic to HTTP, so they can hijack traffic, steal credentials, and deliver malware to the device. **Mitigation**: Automatic **Vector**: Network **Tag**:network.mitm.ssl_strip **MITRE Tactics:** Collection, Exfiltration, Network Effects	Threat	Critical	Yes	Yes	Yes	Yes	Yes	SSL_STRIP, 14

Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
MTD Is Not Activated on Both Work and Personal Profiles – Android Enterprise	The Mobile Threat Defense (MTD) application is not activated on both the personal and work profiles on this device. Install and activate the MTD app in both locations to ensure full device protection. **Mitigation**: Automatic **Vector**: Device **Tag**:host.afw_both_profiles_not_activated **MITRE Tactics:** n/a	Risk	Elevated	Yes	---	n/a	Yes (4.4)	---	ZIPS_NOT_RUNNING_ON_CONTAINER, 78
Network Handoff	A network handoff occurred and can allow a device to alter routing on a network, potentially allowing for a man-in-the-middle attack. **Mitigation**: Automatic **Vector**: Network **Tag**:network.arp.handoff **MITRE Tactics:** Initial Access, Network Effects, Exfiltration	Risk [d]	Normal	Yes (OS<=9)	Yes (OS<=9)	---	Yes	Yes	NETWORK_HANDOFF, 36
Out of Compliance App	One or more apps are found on the device that are marked as Out-of-Compliance apps. **Mitigation**: Automatic **Vector**: Device **Tag**:host.app_out_of_compliance **MITRE Tactics:** Exfiltration, Collection, Impact	Risk	Elevated	Yes	Yes	Yes	Yes (4.9)	Yes (4.9) [h]	OUT_OF_COMPLIANCE_APP, 93

Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
Out of Compliance Browser Extension	A Chrome extension is detected that is marked out of compliance with your organization's policies. It is recommended that you remove it from your Chrome browser. **Mitigation**: Automatic **Vector**: App **Tag**:chromeos.extension.ooc **MITRE Tactics:** n/a **Threat Active Date**: December 2021	Risk	Elevated	—	—	Yes	—	Yes	OOC_BROWSER_EXTENSION, 1003
Over-The-Air (OTA) Updates Disabled	Over-the-air (OTA) updates have been disabled on this device. OTA updates help keep a device's software up to date and more secure. **Mitigation**: Automatic **Vector**: Device **Tag**:host.ota_updates_disabled **MITRE Tactics:** Impact	Risk	Low	Yes	---	Yes	Yes (4.8)	Yes (4.8)	OVER_THE_AIR_UPDATES_DISABLED, 86
Pegasus Spyware	The Pegasus spyware has been detected on the device. Pegasus is a surveillance tool that is used to monitor and collect information from the device. **Mitigation**: Automatic **Vector**: Device **Tag**:host.pegasus **MITRE Tactics:** Initial Access, Command and Control **Threat Active Date**: August 2021	Threat	Critical	---	Yes	---	Yes (4.19)	Yes (4.19)	PEGASUS, 130

Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
Phishing Protection - Link Tapped	A potentially malicious website address (URL) link was tapped on the device. **Mitigation**: Automatic **Vector**: Device **Tag**:host.site-insight.link-tapped **MITRE Tactics:** Initial Access, Credential Access, Network Effects	Risk	Elevated	Yes	Yes	Yes	Yes	Yes [h]	MALICIOUS_WEBSITE, 9
Phishing Protection - Link Visited	A user tapped a potentially malicious URL on the device. The user was warned of potential danger with the linked site, and chose to continue to the website after the warning. **Mitigation**: Automatic **Vector**: Device **Tag**:host.site-insight.link-visited **MITRE Tactics:** Initial Access, Credential Access, Network Effects, Execution, Privilege Escalation	Threat	Critical	Yes	Yes	Yes	Yes	Yes [h]	MALICIOUS_WEBSITE_OPENED, 72
Proxy Change	Proxy configuration changes on the mobile device can be indicative of sending traffic to a non-intended destination. **Mitigation**: Automatic **Vector**: Network **Tag**:host.config.proxy **MITRE Tactics:** Initial Access, Network Effects, Exfiltration	Risk	Low	Yes	---	---	Yes	Yes	PROXY_CHANGE, 15

Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
Risky Site Blocked	A potentially malicious website address (URL) link was blocked on the device. **Mitigation**: Automatic **Vector**: Device **Tag**:content_filter.malsite_blocked **MITRE Tactics:** Initial Access **Threat Active Date**: October 2021	Threat	Elevated	Yes	Yes	Yes	Yes (4.20.4)	---	MAL_WEBSITE_BLOCKED, 137
Risky Site - Link Tapped	A potentially malicious website address (URL) link was tapped on the device. **Mitigation**: Automatic **Vector**: Device **Tag**:content_filter.malsite_tapped **MITRE Tactics:** Initial Access **Threat Active Date**: October 2021	Threat	Elevated	Yes	Yes	Yes	Yes (4.20.4)	---	MAL_WEBSITE_TAPPED, 135
Risky Site - Link Visited	A user tapped a potentially malicious link on the device. The user was warned of potential danger with the linked site, and chose to continue to the website after the warning. **Mitigation**: Automatic **Vector**: Device **Tag**:content_filter.malsite_visited **MITRE Tactics:** Initial Access **Threat Active Date**: October 2021	Threat	Critical	Yes	Yes	Yes	Yes (4.20.4)	---	MAL_WEBSITE_VISITED, 136

Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
Rogue Access Point	Rogue access points exploit a device vulnerability to connect to a previously known Wi-Fi network by masking preferred and known networks. **Mitigation**: Automatic **Vector**: Network **Tag**:network.mitm.rogue_ap **MITRE Tactics:** Network Effects, Initial Access, Credential Access	Threat	Critical	Yes [g]	Yes	Yes	Yes	Yes	ROGUE_ACCESS_POINT, 38
Rogue Access Point: Nearby	Rogue access points exploit device vulnerability to connect to a previously known Wi-Fi network by masking preferred and known networks. **Mitigation**: Automatic **Vector**: Network **Tag**:network.mitm.rogue_ap_nearby **MITRE Tactics:** Initial Access, Network Effects	Risk	Elevated	Yes [g]	---	Yes	Yes	Yes	ROGUE_ACCESS_POINT_NEARBY, 65
SELinux Disabled	Security-enhanced Linux (SELinux) is a security feature in the operating system that helps maintain the operating system's integrity. If SELinux has been disabled, the operating system's integrity may be compromised and should be investigated immediately. **Mitigation**: Automatic **Vector**: Device **Tag**:host.selinux.disabled **MITRE Tactics:** Impact	Threat	Critical	Yes	---	---	Yes	Yes	SELINUX_DISABLED, 61

Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
Sideloaded App(s)	Sideloaded apps are installed independently of an official app store and can present a security risk. **Mitigation**: Automatic **Vector**: App **Tag**:host.sideloaded_app **MITRE Tactics:** Initial Access, Collection, Exfiltration, Persistence	Risk	Elevated	Yes	Yes	Yes	Yes (4.7)	Yes (4.7)	SIDELOADED_APP, 76
Sideloaded Browser Extension	A sideloaded extension is detected, which was not installed from an official web store. These extensions and their developers may not be verified and can present a security risk. **Mitigation**: Automatic **Vector**: App **Tag**:chromeos.extension.sideloaded **MITRE Tactics:** n/a **Threat Active Date**: December 2021	Risk	Elevated	—	—	Yes	—	Yes	SIDELOADED_BROWSER_EXTENSION, 1005
Site Blocked	A user tapped on website content not approved by your organization and the site was blocked. **Mitigation**: Automatic **Vector**: Device **Tag**:content_filter.blocked **MITRE Tactics:** Initial Access **Threat Active Date**: October 2021	Risk	Elevated	Yes	Yes	Yes	Yes (4.20.4)	---	WEBSITE_BLOCKED, 134

Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
Site Warning - Link Tapped	Website content not approved by your organization was tapped on the device. **Mitigation**: Automatic **Vector**: Device **Tag**:content_filter.website_tapped **MITRE Tactics:** Initial Access **Threat Active Date**: October 2021	Risk	Elevated	Yes	Yes	Yes	Yes (4.20.4)	---	WEBSITE_TAPPED, 132
Site Warning - Link Visited	A user tapped on website content not approved by your organization. The user was warned the website content does not comply with your organization's policies and chose to continue to the website after the warning. **Mitigation**: Automatic **Vector**: Device **Tag**:content_filter.website_visited **MITRE Tactics:** Initial Access **Threat Active Date**: October 2021	Risk	Elevated	Yes	Yes	Yes	Yes (4.20.4)	---	WEBSITE_VISITED, 133
SSL/TLS Downgrade	SSL/TLS downgrades force apps to use old encryption protocols. These protocols may be vulnerable to attacks that allow third parties to view encrypted information. **Mitigation**: Automatic **Vector**: Network **Tag**:network.ssl_tls_downgrade **MITRE Tactics:** Impact, Network Effects	Threat	Low	Yes	Yes	---	Yes (4.4)	Yes (4.4)	TLS_DOWNGRADE, 77

Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
Stagefright Vulnerability	Stagefright vulnerability indicates the device is on an OS patch version susceptible to compromise. **Mitigation**: Automatic **Vector**: Device **Tag**:host.mediaserver.sf_vulnerability **MITRE Tactics:** Impact	Risk	Elevated	Yes	---	Yes	Yes	Yes	STAGEFRIGHT_VULNERABLE, 40
Suspicious Android App	A known malicious app attempts to control the device in some manner, such as elevation of privileges or spyware. **Mitigation**: Automatic **Vector**: App **Tag**:host.app.malicious **MITRE Tactics:** Initial Access, Persistence, Exfiltration, Impact, Credential Access, Execution, Collection	Threat	Critical	Yes	---	Yes	Yes	Yes	APK_SUSPECTED, 13
Suspicious Browser Extension	An unsafe extension is detected. It is strongly recommended that you remove the extension immediately. **Mitigation**: Automatic **Vector**: App **Tag**:chromeos.extension.suspicious **MITRE Tactics:** n/a **Threat Active Date**: December 2021	Threat	Critical	—	—	Yes	—	Yes	SUSPICIOUS_BROWSER_EXTENSION, 1002

Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
Suspicious iOS App	A known malicious app is detected and can attempt to take control of the device in some manner, such as elevation of privileges or spyware. **Mitigation**: Automatic **Vector**: App **Tag**:host.ipa.malicious **MITRE Tactics:** Initial Access, Persistence, Exfiltration, Impact, Credential Access, Execution, Collection	Threat	Critical	---	Yes [b]	n/a	Yes	Yes [h]	SUSPICIOUS_IPA, 42
Suspicious Profile	A suspicious profile is a new profile introduced into the environment and is not explicitly trusted or untrusted. An administrator must review the profile and mark the profile as trusted or untrusted. **Mitigation**: Automatic **Vector**: Device **Tag**:host.profile.suspicious **MITRE Tactics:** Initial Access, Persistence, Exfiltration, Impact, Credential Access, Execution, Collection	Risk	Elevated	---	Yes [b]	n/a	Yes	---	SUSPICIOUS_PROFILE, 45

Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
System Tampering	System tampering is a process of removing security limitations that are in place by the device manufacturer, and it indicates that the device is fully compromised and can no longer be trusted. **Mitigation**: Manual **Vector**: Device **Tag**:host.systemconfig.system_tampering **MITRE Tactics:** Execution, Privilege Escalation, Impact	Threat	Critical	Yes	Yes	Yes	Yes	Yes	SYSTEM_TAMPERING, 37
TCP Scan	A reconnaissance scan using the TCP protocol is often an indicator of a malicious attacker searching for a device vulnerable to a network attack, such as MITM. **Mitigation**: Automatic **Vector**: Network **Tag**:network.scan.tcp **MITRE Tactics:** Initial Access, Discovery, Collection, Network Effects	Risk	Normal	Yes (OS<=9)	Yes (OS<=9)	---	Yes	Yes	TCP_SCAN, 0

Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
UDP Scan	A reconnaissance scan using the UDP protocol is often an indicator of a malicious attacker searching for a device vulnerable to a network attack, such as MITM. **Mitigation**: Automatic **Vector**: Network **Tag**:network.scan.udp **MITRE Tactics:** Initial Access, Discovery, Collection, Network Effects	Risk	Normal	Yes (OS<=9)	Yes (OS<=9)	---	Yes	Yes	UDP_SCAN, 1
Unknown Sources Enabled	App downloads from locations other than the Google Play store are enabled. **Mitigation**: Automatic **Vector**: Device **Tag**:host.config.unknown_sources **MITRE Tactics:** Impact, Initial Access	Risk	Elevated	Yes (OS<=7)	---	Yes	Yes	Yes	UNKNOWN_SOURCES_ON, 25
Unsecured Wi-Fi Network	A connection to an unsecured Wi-Fi network is detected, and these networks are not protected by encryption or authentication protocols and are open to attackers. **Mitigation**: Automatic **Vector**: Network **Tag**:network.unsecured.wifi **MITRE Tactics:** Initial Access, Network Effects, Exfiltration, Collection	Risk	Low	Yes	Yes[a]	---	Yes	Yes[a]	UNSECURED_WIFI_NETWORK, 66

Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
Untrusted Profile	An untrusted profile is a profile installed on one or more devices and is unsafe on your devices. An untrusted profile installed on devices can be used to control devices remotely, monitor and manipulate user activities, and hijack users' traffic. **Mitigation**: Automatic **Vector**: Device **Tag**:host.profile.untrusted **MITRE Tactics:** Initial Access, Persistence, Exfiltration, Impact, Credential Access, Execution, Collection	Threat	Critical	---	Yes [b]	n/a	Yes	Yes [h]	UNTRUSTED_PROFILE, 24
USB Debugging Mode	USB debugging is an advanced configuration option intended for development purposes only. By enabling USB debugging, your device can accept commands from a computer when plugged into a USB connection. **Mitigation**: Automatic **Vector**: Device **Tag**:host.usb.debugging **MITRE Tactics:** Impact, Initial Access	Risk	Elevated	Yes	---	Yes	Yes	Yes	USB_DEBUGGING_ON, 44

Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
Vulnerable Android Version	The Android version installed on the device is not up to date. The outdated operating system exposes the device to known vulnerabilities and the threat of being exploited by malicious actors. You need to update the operating system immediately. **Mitigation**: Automatic **Vector**: Device **Tag**:host.vulnerable.android **MITRE Tactics:** Impact	Risk	Elevated	Yes	---	Yes	Yes	Yes	ANDROID_NOT_UPDATED, 51
Vulnerable iOS Version	The iOS version installed on the device is not up to date. The outdated operating system exposes the device to known vulnerabilities and the threat of being exploited by malicious actors. You need to update the operating system immediately. **Mitigation**: Automatic **Vector**: Device **Tag**:host.vulnerable.ios **MITRE Tactics:** Impact	Risk	Elevated	---	Yes	n/a	Yes	Yes	IOS_NOT_UPDATED, 52
Vulnerable, Non-Upgradable Android Version	The device is running a vulnerable Android version. However, the device is not eligible for an operating system upgrade at this time. **Mitigation**: Automatic **Vector**: Network **Tag**:host.vulnerable.android.non-upgradeable **MITRE Tactics:** Impact	Risk	Low	Yes	---	Yes	Yes (4.4)	Yes (4.4)	VULNERABLE_NON_UPGRADEABLE_ANDROID_VERSION, 89

Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
Vulnerable, Non-Upgradable iOS Version	The device is running a vulnerable iOS version. However, the device is not eligible for an operating system upgrade at this time. **Mitigation**: Automatic **Vector**: Network **Tag**:host.vulnerable.ios.non-upgradeable **MITRE Tactics:** Impact	Risk	Low	---	Yes	n/a	Yes (4.4)	Yes (4.4)	VULNERABLE_NON_UPGRADEABLE_IOS_VERSION, 88