NOLIA

VULNERABILITY DISCLOSURE

ROOMCAST TA-2400 BY TELEADAPT

OVERVIEW

During our comprehensive evaluation of the RoomCast TA-2400, we have discovered multiple vulnerabilities that span across the various nodes comprising the RoomCast system. These nodes include the Google Chromecast node, the Android node, and the OpenWRT node, each playing a crucial role in the overall functionality of the RoomCast device.

The Google Chromecast node acts as a media streaming device, allowing users to cast content from their smartphones, tablets, or computers to a television or audiovisual system. It provides seamless integration with popular streaming platforms, enhancing the entertainment experience within hotel rooms or other hospitality settings.

The Android node, another integral component of the RoomCast system, serves as an operating system at it's core. The main use of the Android node is to host an Android Package (APK) which provides the users/ guests a graphical user interface for the RoomCast system.

The OpenWRT node functions as the networking component of the RoomCast TA-2400. It facilitates connectivity, network management, and communication between the device and other networked devices within the premises. The OpenWRT node plays a vital role in ensuring seamless streaming, data transfer, and overall network performance.

During our investigative stage, driven by the desire to thoroughly evaluate the RoomCast TA-2400 device and identify any security issues, we meticulously analyzed each of these nodes. In doing so, we uncovered several vulnerabilities that require attention to ensure the continued security and reliability of the RoomCast system.

In the following sections, we will provide a detailed overview of the vulnerabilities discovered across the RoomCast system and it's nodes, along with recommendations for mitigation and potential security enhancements.

VERSION DISCLAIMER

Despite our limited access to specific versions, it is crucial to highlight that our testing encompassed every version of the RoomCast device available to us. Notably, we found that each version examined was susceptible to the identified vulnerabilities. These critical flaws extend to RoomCast devices running the documented versions 2.0 and 3.0, as well as custom releases of the RoomCast software that were pre-installed on certain devices, which our team has classified 3.1+.

The wide-ranging impact of these vulnerabilities across all tested versions underscores the urgency with which these vulnerabilities should be addressed. Regardless of the specific iteration or the inclusion of customized software, the fundamental security flaws persists. This revelation necessitates immediate attention to fortify the RoomCast ecosystem. By doing so, TeleAdapt can safeguard the security and integrity of RoomCast devices across their entire user base, providing peace of mind to consumers irrespective of the version they utilize.

The versions our team has evaluated are as follows;

RoomCast Release 2.00
Android Node: 5.1.1 – 2016-06-14
RoomCast APK - 7.3.17032921
Chromecast Node- 1.56.275994
OpenWRT Node - qsdk_170322

RoomCast Release 3.00
Android Node: 5.1.1 – 2016-06-14
RoomCast APK - 7.3.17090818
Chromecast Node- 1.56.275994
OpenWRT Node - qsdk_170622

RoomCast Release 3.1+
Android Node: 5.1.1 – 2016-06-14
RoomCast APK: 7.3.17113016
Chromecast Node- 1.56.275994
OpenWRT Node: qsdk_171031

RoomCast Release 3.1+
Android Node: 5.1.1 – 2016-06-14
RoomCast APK: 7.3.19062719
Chromecast Node- 1.56.275994
OpenWRT Node: qsdk_190420

COMMON TERMS/ABBREVIATIONS

NOLIA

CWE - Common Weakness Enumeration

APK - Android Package

CVSS - Common Vulnerability Scoring System

ADB - Android Debug Bridge

RSA - Rivest-Shamir-Adleman

CAPI - ChromeCast Application Programming Interface

PAN - Private Area Network

LAN - Local Area Network

VPN - Virtual Private Network

GUI - Graphical User Interface

POC - Proof of Concept

OS - Operating System

CWE-318 - OVERVIEW

OpenWRT

CVE—2023-33742: CLEARTEXT STORAGE OF SENSITIVE INFORMATION IN EXECUTABLE in UPDATE.EXE in TELEADAPT ROOMCAST TA-2400 1.0.0 AND LATER allows REMOTE ATTACKERS to GET ROOT SHELL via SSH AUTHENTICATION

Vulnerabilty Type: CWE-318: Cleartext Storage of Sensitive Information in Executable

Vulnerabilty Description: The Update.exe file exposes the RSA private key used for authentication with the OpenWRT node. This unencrypted RSA private key can be extracted from the Update.exe file, enabling an unauthorized individual to establish a root-level SSH connection with the OpenWRT node.

Software: Update.exe

RoomCast System Component: OpenWRT

CVSS Base Score: Critical Risk - 9.6
CVSS Temporal Score: Critical Risk - 9.1
CVSS v3.1 Vector: AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:F/RL:W/RC:C

Exploitability Metrics:
Attack Vector (AV): Adjacent Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Changed

Impact Metrics:
Confidentiality Impact (C): High
Integrity Impact (I): High
Availability Impact (A): High

Temporal Score Metrics:
Exploit Code Maturity (E): Functional Exploit Exists
Remediation Level (RL): Workaround
Report Confidence (RC): Confirmed

Impact statements on next page

Confidentiality Metric: HIGH

The CWE-318 vulnerability, which involves the disclosure of the RSA private key, poses a significant risk to confidentiality, warranting a High severity rating. Exploiting this vulnerability grants an attacker root access to the OpenWRT node, enabling them to gain complete control over the device. Consequently, the attacker can freely access and retrieve the entire configuration setup stored on the OpenWRT node.

Moreover, the exploitation of this vulnerability allows the attacker to monitor and log all network traffic passing through the compromised OpenWRT node. By assuming control over the node, the attacker can intercept sensitive information, jeopardizing the confidentiality of both the OpenWRT router and all data transmitted through the node. The impact of this vulnerability extends beyond the device itself, compromising the confidentiality of users' data traversing the RoomCast network.

Integrity Metric: HIGH

The CWE-318 vulnerability, involving the disclosure of the RSA private key, poses a significant risk to integrity, warranting a High severity rating. Exploiting this vulnerability grants an attacker root access to the OpenWRT node, granting them unrestricted control which allows an attacker to modify the system configuration.

By gaining root access through this vulnerability, an attacker can modify any aspect of the OpenWRT node. This compromises the integrity of the device and raises concerns about the trustworthiness of the settings intended to protect users' devices. A guest utilizing the RoomCast device has no means of discerning whether the configuration on the OpenWRT node is designed to safeguard their interests or maliciously exploit them.

An attacker can exploit this vulnerability to establish new gateway and proxy settings on the OpenWRT node, redirecting all user traffic to a malicious server of their choosing. This manipulation of network settings allows the attacker to intercept and manipulate data transmitted through the RoomCast device, severely compromising the integrity of the entire system.

Continued on next page

Availability Metric: HIGH

The CWE-318 vulnerability, involving the disclosure of the RSA private key, poses a significant risk to availability, warranting a High severity rating. Exploiting this vulnerability grants an attacker root access to the OpenWRT node, enabling them to disrupt service.

With root access obtained through this vulnerability, an attacker can effortlessly modify the router configuration, leading to the obstruction of traffic passing through the OpenWRT node. By tampering with the LAN network or disabling the WAN interface, an attacker can effectively prevent any data from traversing through the device. Additionally, the attacker can apply rate limiting measures to degrade the user experience or alter DHCP settings, resulting in a loss of network connectivity for other components within the RoomCast system.

Furthermore, an attacker with root access can inflict permanent damage on the RoomCast device by corrupting the firmware. By making intentional modifications to the OpenWRT component, an attacker can render the RoomCast completely unusable. This extensive control over the device enables the attacker to disrupt almost all services provided by the RoomCast, significantly impacting its availability and utility.

End of Impact Statements

CWE-318 - PROOF

OpenWRT

In this section, we present a detailed proof of concept (PoC) to illustrate the identified vulnerability within the RoomCast TA-2400 device. The PoC provides step-by-step instructions for identifying the vulnerability and successfully exploiting it. It is important to note that for testing the PoC, we recommend using a Linux-based environment, which offers the necessary tools and compatibility for conducting the tests accurately and reliably.

1. Download the latest OpenWRT firmware package from the RoomCast support page.
   Support Portal: https://rc.teleadapt.com
   Download: https://rc.teleadapt.com/roomcast/production/releases/r3.00/router_firmware_170622.zip

2. Open the firmware archive that was previously downloaded and locate the update.exe file.

3. Extract the RSA private key from the update.exe executable and save it to a local private key file.
   Navigate to the location of the update.exe file from step 1 and 2 and run the following command;

strings update.exe | sed -n "$(strings update.exe | grep -n -e "BEGIN RSA PRIVATE KEY" | cut -d : -f 1),$(strings update.exe | grep -n -e "END RSA PRIVATE KEY" | cut -d : -f 1)p" | sed "s/--t/--/g" > rsa_key.pem

4. Change the permissions of the newly saved rsa_key.pem file so it can work with the ssh command.
   Run the following command;

sudo chmod 400 rsa_key.pem

5. Establish an SSH connection with the OpenWRT node. Run the following command while being in the same directory as the created rsa_key.pem file.

sudo ssh -o KexAlgorithms=diffie-hellman-group1-sha1 -o HostKeyAlgorithms=ssh-rsa -o PubkeyAcceptedKeyTypes=ssh-rsa -i rsa_key.pem root@192.168.20.1

If this is your first time connecting to the OpenWRT node you will need to confirm this as a verified host.

You should now have a terminal session on the OpenWRT node as **root** user. This is a completed compromise of the OpenWRT node, providing unrestricted control over its operations and configurations.

CWE-318 - RISK SUMMARY

OpenWRT

The exposure of the private RSA key facilitates the establishment of a root shell on the OpenWRT node via SSH, resulting in a complete compromise of the device's security. Once an attacker gains root access, they possess unrestricted control and can execute various actions within the compromised environment. These actions include, but are not limited to:

1. Resetting the web root password to the OpenWRT router: The attacker can change the administrative password, effectively locking out legitimate users and assuming complete control over the device.

2. Stealing user data: With root access, the attacker can access and exfiltrate sensitive user information, compromising their privacy and potentially leading to identity theft or unauthorized access to personal accounts.

3. Taking complete control of the wireless network and connected devices: The attacker can manipulate network settings, intercept or modify network traffic, and gain unauthorized access to devices connected to the network.

4. Making configuration changes: The attacker can modify various device configurations, potentially enabling them to introduce malicious settings, redirect network traffic, or compromise the integrity of the network.

5. Setting up poisoned DNS services and proxies: The attacker can deploy malicious DNS servers or proxies, redirecting network traffic to malicious websites or intercepting sensitive data transmitted over the network.

6. Setting up malicious captive portals: By configuring deceptive captive portals, the attacker can trick users into entering their credentials or installing malicious software, further compromising their security.

7. Disabling the device by corrupting the node firmware: The attacker can intentionally corrupt the firmware of the OpenWRT node, rendering the device inoperable and disrupting its functionality.

The presence of the CWE-318 vulnerability allows an attacker to wield extensive control over the RoomCast device, jeopardizing user data, network integrity, and device functionality. Urgent remediation of this vulnerability is essential to mitigate these risks and safeguard the device and its users from potential harm.

CWE-269, 284 - OVERVIEW

Android

CVE—2023-33743: IMPROPER ACCESS CONTROL in ANDROID NODE in TELEADAPT ROOMCAST TA-2400 1.0.0 AND LATER allows REMOTE ATTACKERS to GET USER SHELL via ANDROID DEBUG BRIDGE

CVE—2023-33745: IMPROPER PRIVILEGE MANAGEMENT in ANDROID NODE in TELEADAPT ROOMCAST TA-2400 1.0.0 AND LATER allows LOCAL to ROOT ELEVATION via ANDROID SHELL

Vulnerabilty Type: CWE-269: Improper Privilege Management
CWE-284: Improper Access Control

Vulnerabilty Description: The Android component of the RoomCast device, specifically the Android fork of Lollipop 5.1.1, presents a notable vulnerability: the Android Debug Bridge (ADB) has been left open. This configuration allows an attacker to establish a shell on the Android node without requiring any authentication. Once a shell is successfully accessed, the attacker can exploit improper privilege management, effortlessly elevating their privileges to root.

Software: Android Lollipop 5.1.1 fork

RoomCast System Component: Android

CVSS Base Score: Critical Risk - 9.6
CVSS Temporal Score: Critical Risk - 9.1
CVSS v3.1 Vector: AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:F/RL:W/RC:C

Exploitability Metrics:
Attack Vector (AV): Adjacent Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Changed

Impact Metrics:
Confidentiality Impact (C): High
Integrity Impact (I): High
Availability Impact (A): High

Temporal Score Metrics:
Exploit Code Maturity (E): Functional Exploit Exists
Remediation Level (RL): Workaround
Report Confidence (RC): Confirmed

Confidentiality Metric: HIGH

The combination of the CWE-284 and CWE-269 vulnerabilities results in a High confidentiality metric for this particular vulnerability. With root privileges, the attacker gains unrestricted access to the entire contents of the Android node. This access enables the attacker to export any desired files, facilitating their dissemination to other locations.

Moreover, the attacker can export the complete Roomcast APK, potentially leading to the decompilation of its source code, allowing for theft of sensitive intellectual property. With root access obtained through this vulnerability, confidentiality cannot be maintained on the Android node, as the attacker possesses unrestricted control over its contents.

Integrity Metric: HIGH

The combination of the CWE-284 and CWE-269 vulnerabilities results in a High integrity metric for this particular vulnerability. Exploiting both vulnerabilities allows an attacker to gain root access to the Android node. This level of access empowers the attacker to modify any aspect of the RoomCast application, potentially altering its entire functionality.

In exploiting these vulnerabilities, an attacker could upload their own pages for the RoomCast to load or manipulate existing pages. This manipulation could include the serving of malicious links or unauthorized content to guests using the RoomCast device. Such unauthorized modifications compromise the integrity of the RoomCast device, as the attacker can wield significant control over its functionalities and the user experience.

Availability Metric: HIGH

The combination of the CWE-284 and CWE-269 vulnerabilities yields a High availability metric for this specific vulnerability. With root privileges, the attacker gains the ability to modify various configuration settings on the Android node, which can result in significant disruptions to availability.

By tampering with the network settings on the Android node, an attacker could render the node unreachable by the OpenWRT component. This would effectively halt all outgoing traffic, breaking the casting functionality of the RoomCast application.

Furthermore, with root access, the attacker could uninstall the RoomCast package entirely from the Android node, rendering the device inoperable upon reboot. This level of access grants the attacker the capability to make the RoomCast completely unusable and potentially cause permanent damage, including corrupting the Android node firmware. Such actions would result in the unavailability of almost all services provided by the RoomCast device.

CWE-269, 284 - PROOF

Android

In this section, we present a detailed proof of concept (PoC) to illustrate the identified vulnerability within the RoomCast TA-2400 device. The PoC provides step-by-step instructions for identifying the vulnerability and successfully exploiting it. It is important to note that for testing the PoC, we recommend using a Linux-based environment, which offers the necessary tools and compatibility for conducting the tests accurately and reliably.

1. Connect your host device to the RoomCast network using either the Ethernet **LAN1** port or by connecting to the wireless network created by RoomCast system.

2. Utilize a network scanning tool such as **nmap** to scan the local network and identify the IP address of the Android node. Run the following command to scan the specific RoomCast network subnet;

sudo nmap 192.168.20.0/24

3. Evaluate the scan results from step 2 and locate the IP address of the Android node. In your scan results, the Android node should be the result with port **5555** open. Additionally, the name of the Android node follows a pattern similar to **“android-xxxxxxxxxxxx.lan”**.

4. Establish a connection to port **5555** on the Android node by using a common linux command line tool named “**adb**”. Run the following command; For this example, the Android node IP address is 192.168.20.123

sudo adb connect 192.168.20.123

5. Once a connection has been established in step 4, run the following command to gain a non-root shell on the Android node;

sudo adb shell

6. Elevate your current shell privileges but becoming a root user with the following command;

su

Now, the terminal session is running with root privileges, granting you full and complete access to the Android node. This represents a completed compromise of the Android node, providing unrestricted control over its operations and configurations.

CWE-269, 284 - RISK SUMMARY

Android

By default, the Android Debug Bridge (ADB) port does not require any authentication, allowing anyone on the network to establish an interactive shell on the Android node. Once a shell is successfully established, an attacker can effortlessly escalate the privileges of the shell to root, taking advantage of improper privilege management. This represents a complete compromise of the Android node, granting the attacker unrestricted control.

With root access on the Android node, the attacker gains the capability to perform a wide range of actions, including but not limited to:

1. Stealing source code and user data: The attacker can access and exfiltrate sensitive source code and user data, potentially leading to intellectual property theft and compromising user privacy.

2. Modifying the RoomCast application: With full access to the Android node, the attacker can modify the RoomCast application, altering its functionalities, introducing malicious code, or manipulating user experiences.

3. Uninstalling core applications: The attacker can remove essential core applications from the Android node, potentially disrupting its normal operation and causing instability.

4. Hosting malware on the Android node: The attacker can deploy and host malicious software or scripts on the compromised Android node, further compromising the integrity of the device and potentially infecting other devices on the network.

5. Installing Malicious APKs on the node: With full control over the Android node, the attacker can install and execute malicious APKs (Android application packages), introducing additional threats or exploiting vulnerabilities within the system.

6. Utilizing the Android device and network to launch other attacks: The compromised Android node can serve as a launchpad for further attacks on the device itself or other devices connected to the network, potentially escalating the scope and impact of the attacker's activities.

The presence of the CWE-269 and CWE-284 vulnerabilities allows an attacker to wield extensive control over the RoomCast device, jeopardizing system data, application integrity, and device functionality. Urgent remediation of this vulnerability is essential to mitigate these risks and safeguard the device and its users from potential harm.

CWE-259 - OVERVIEW

RoomCast Android Package

CVE—2023-33744: USE OF HARD-CODED PASSWORD in ROOMCAST.APK in TELEADAPT ROOMCAST TA-2400 1.0.0 AND LATER allows LOCAL to AUTHENTICATE via MANAGEMENT MODE

Vulnerabilty Type: CWE-259: Use of Hard-coded Password

Vulnerabilty Description: The RoomCast application encompasses three distinct management modes: Hotel mode, Admin mode, and Engineering mode. Notably, the passwords for all three management portals are publicly available and documented as part of the RoomCast documentation. It is important to note that the owners of the device do not have the ability to modify these passwords. Among the three modes, the Engineering mode holds the greatest impact. This powerful mode allows for modifications to be made to the Android component, as well as the initiation of a terminal session on the Android node.

Software: Roomcast.apk

RoomCast System Component: Android

CVSS Base Score: Medium Risk - 5.9
CVSS Temporal Score: Medium Risk - 5.8
CVSS v3.1 Vector: AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:F/RL:U/RC:C

Exploitability Metrics:
Attack Vector (AV): Local
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Unchanged

Impact Metrics:
Confidentiality Impact (C): Low
Integrity Impact (I): Low
Availability Impact (A): Low

Temporal Score Metrics:
Exploit Code Maturity (E): Functional Exploit Exists
Remediation Level (RL): Unavailable
Report Confidence (RC): Confirmed

Impact statements on next page

Confidentiality Metric: LOW

The Confidentiality metric for the CWE-259 vulnerability in question is assessed as Low. While accessing the management modes does provide access to certain information that may not be intended for standard users, the disclosure of confidential data is relatively limited. Within the Admin mode, access to network configuration settings, which may be considered confidential information, is possible. Similarly, in the Engineering mode, interaction with the Android node GUI can potentially reveal confidential details such as the Android Build number, latest updates, app usages, and other sensitive files.

Nevertheless, the extent of confidential information that can be leaked due to this vulnerability remains restricted, resulting in a Low impact metric for confidentiality.

Integrity Metric: LOW

The Integrity metric for the CWE-259 vulnerability under consideration is classified as Low. This assessment is based on the fact that the permissions granted through accessing the management modes align with the intended functionality of those consoles. While accessing the management consoles does provide an attacker with the ability to modify certain application settings, the impact of these changes is limited to the capabilities already intended by the respective management consoles.

Within the Admin mode, settings related to network configuration, CAPI setup, PAN setup, and other parameters that can potentially impact the integrity of the RoomCast can be altered. Similarly, in the Engineering mode, an attacker can access the Android node and carry out modifications such as installing additional applications, altering existing applications, and editing internal Android OS settings like Proxy and VPN configurations.

Overall, while this vulnerability has implications for the integrity of the RoomCast device, its impact is confined to the boundaries defined by the management modes, resulting in a Low impact metric for Integrity.

Continued on next page

Availability Metric: LOW

The Availability metric for the CWE-259 vulnerability being discussed is classified as Low. This determination is based on the fact that the permissions granted through accessing the management modes align with the intended functionality of those consoles. While accessing the management consoles does provide an attacker with the ability to modify certain application settings, the impact of these changes is limited to the capabilities already intended by the respective management consoles.

Within the Admin mode, settings such as network configuration and other parameters can be altered, potentially impacting the availability of the RoomCast application. Misconfigurations of these settings can lead to disruptions that prevent the RoomCast from functioning properly.

While this vulnerability has implications for the availability of the RoomCast application, its impact is limited to the abilities intended by the management consoles, resulting in a Low impact metric for Availability.

End of Impact Statements

In this section, we present a detailed proof of concept (PoC) to illustrate the identified vulnerability within the RoomCast TA-2400 device. The PoC provides step-by-step instructions for identifying the vulnerability and successfully exploiting it.

1. In the RoomCast graphical user interface navigate to the About/Feedback page using the RoomCast provided remote.

2. Enter in the combination of feedback levels (outlined below) to enter the different management modes.

Connect to the **Hotel** management mode;
Select the feedback level **“Struggled”, “Struggled”**.
Enter the password/PIN: **385521**

Connect to the **Admin** management mode;
Select the feedback level **“Struggled”, “Struggled”**.
Enter the password/PIN: **843646**

Connect to the **Engineering** management mode;
Select the feedback level **“Not Cool”, “Whatever”, “Love It”**.
Enter the password/PIN: **592671**

Following these recreation steps will enable you to access the respective management modes within the RoomCast device, allowing you to utilize the associated functionalities and features.

CWE-259 - RISK SUMMARY

RoomCast Android Package

The current design of the RoomCast management modes lacks the capability for owners or administrators to modify the default passwords associated with these modes. Consequently, anyone can easily access the management modes by obtaining the default passwords. This unrestricted access opens up various possibilities, including but not limited to:

1. Reading system configuration settings: Users with access to the management modes can view and gather information regarding system configurations, potentially revealing sensitive details about the RoomCast device.

2. Changing network configurations: Unauthorized individuals can modify network settings within the management modes, potentially causing disruptions to the network connectivity of the RoomCast device or altering its intended functionality.

3. Changing Android node settings: The management modes provide the ability to modify settings related to the Android node, allowing unauthorized individuals to manipulate its configurations or behavior.

4. Installing apps on the Android node: Users with access to the management modes can install additional applications on the Android node, potentially introducing malicious software or compromising the stability and security of the device.

5. Accessing the Android GUI or shell: Unauthorized access to the management modes grants individuals the ability to interact with the Android node's graphical user interface (GUI) or gain access to the shell, providing them with a level of control over the device beyond what is intended for regular users.

The presence of the CWE-259 vulnerability enables unauthorized users to access the RoomCast device, impacting system data, application integrity, and device functionality. Remediation of this vulnerability is recommend in order to mitigate these risks and safeguard the device and its users from potential harm.

Disclaimer: We would like to highlight that the mitigation methods provided over the next few pages are temporary workarounds that we have identified to address the specific attack vectors discussed in this report. However, it is important to note that these measures should not be interpreted as permanent or production-ready solutions. Implementation of these mitigation steps may have lasting side-effects and may not be suitable for every use case or environment. We cannot guarantee their effectiveness or compatibility in all scenarios. Therefore, it is crucial for TeleAdapt to conduct a thorough evaluation and consider their specific requirements when devising permanent solutions to address the identified vulnerabilities.

A quick workaround for addressing the CWE-318 vulnerability involves disabling the Dropbear service running on the OpenWRT router. Dropbear is responsible for the SSH capabilities utilizing port 22. By disabling the service, port 22 becomes closed and inaccessible for authentication. Consequently, the exposed RSA private key becomes useless, preventing unauthorized access to the OpenWRT node.

1. Disable Dropbear: The Dropbear service can be disabled through the OpenWRT administration web portal.

It's important to consider that this workaround has a significant side effect: the current documented methods for applying updates to the OpenWRT node will no longer work. To install new updates, it will be necessary to manually re-enable the Dropbear service on the OpenWRT node. Although this approach effectively mitigates the immediate risks associated with the vulnerability, it does hinder the regular update process.

Continued on next page

CWE-269, 284 - HOTFIX

Android

A quick workaround for addressing the CWE-284 vulnerability involves disabling the Android Debug Bridge (ADB) service running on the Android node. The Android Debug Bridge service is responsible for utilizing port 5555. By disabling the ADB service, port 5555 will be closed. This will prevent any unauthenticated connections from being established utilizing ADB.

In order to address the CWE-269 vulnerability proper authentication mechanisms need to be put in place, preventing the elevation of privileges without appropriate authentication credentials.
This ensures that only authorized users can access and perform actions with elevated privileges. This can be done by creating passwords for root users

1. Disable Android Debug Bridge: The ADB service can be disabled utilizing the Android terminal which is accessible from the the RoomCasts Engineering mode.

2. Create root password: A password can be created for the root user by utilizing the Android terminal which is accessible from the the RoomCast's Engineering mode.

Disabling the ADB service significantly reduces the potential for unauthorized access and adding passwords for root users greatly increases the security of those accounts

Continued on next page

Unfortunately, based on our research there is not a quick way to implement a workaround to avoid this CWE-259 vulnerability without modifying the source code of the RoomCast application. To effectively mitigate the CWE-259 vulnerability, the following recommended mitigation steps should be implemented:

1. Implement password customization: Provide administrators and owners with the ability to change the passwords associated with the Management Modes. By enabling password customization, default passwords become obsolete, significantly reducing the risk of unauthorized access. This allows administrators to establish unique and secure passwords, enhancing the overall security of the RoomCast device.

2. Disable Engineering mode: Evaluate the specific requirements and use cases of the RoomCast device to determine if Engineering mode is essential for standard administration and configuration needs. If Engineering mode is not necessary, consider implementing a feature that allows administrators to disable it entirely. By disabling this mode, potential risks and vulnerabilities associated with Engineering mode are mitigated, reducing the attack surface and enhancing the security posture of the device.

By implementing these mitigation steps, TeleAdapt can strengthen the security of the RoomCast device, significantly reducing the potential for unauthorized access, misuse, and exploitation.

End of workarounds