|  |  |
| --- | --- |
| Product name | Confidentiality level |
| HEY2-W09 | CONFIDENTIAL |
| Commercial Name | Total 8 pages |
| HONOR Pad 9 |

**HEY2-W09 8.0.0.208(C636E147R2P1)**

**Software Release Notes**

|  |  |  |  |
| --- | --- | --- | --- |
| Prepared by | HEY2 Team | Date | 2025-03-06 |
| Reviewed by | HEY2 Team | Date | 2025-03-06 |
| Approved by | HEY2 Team | Date | 2025-03-06 |

All rights reserved

Revision Record

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Revision version | Change Description | Author |
| 2025-03-06 | 1.0 | First draft | HEY2 Team |

Table of Contents

[1 Version Description 4](#_Toc191569267)

[2 New Features 4](#_Toc191569268)

[3 Improvement from the Previous Version 4](#_Toc191569269)

[4 Known Limitations and Issues 4](#_Toc191569270)

[5 Software Vulnerabilities Fixes 4](#_Toc191569271)

**HEY2-W09 8.0.0.208(C636E147R2P1)**

**Software Release Notes**

# Version Description

|  |  |
| --- | --- |
| Model | HEY2-W09 |
| Build number | 8.0.0.208(C636E147R2P1) GPU Turbo |
| Previous released number | 8.0.0.204(C636E147R2P1) GPU Turbo |
| IMEI SV | NA |
| Android version | 14 |
| Magic version | 8.0 |
| CPU | Snapdragon® 6 Gen 1 Mobile Platform |
| Android security patch | March 1,2025 |
| Baseband version | NA |
| Kernel Version | 5.10.209-android12-9-00021-g591df1b05194-ab12385099 build-user@build-host #1 Mon Sep 2 13:26:35 UTC 2024 |
| Version Type | Google Patch MR |

# New Features

| **Index** | **Feature Description** |
| --- | --- |
| 1 | Updated to Android March 2025 security patch to enhance system security. |

# Improvement from the Previous Version

| **Index** | **Issue Description** |
| --- | --- |
| 1 | NA |

# Known Limitations and Issues

| **Index** | **Issue Description** | **Remarks** |
| --- | --- | --- |
| 1 | NA |  |

# Software Vulnerabilities Fixes

Vulnerabilities information is available through CVE IDs in NVD (National Vulnerability Database) website: <http://web.nvd.nist.gov/view/vuln/search>

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Software/Module name | Version | CVE ID | Vulnerability Description | Impact Description |
| Platform | 12,12L,13,14,15 | CVE-2024-49743 | In multiple locations, there is a possible way to launch an activity from the background due to BAL Bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. | The fix is designed to ensure the notification service has the correct token. |
| Platform | 12,12L,13,14,15 | CVE-2024-49746 | In multiple functions of Parcel.cpp, there is a possible way to manipulate file descriptors and escalate privileges due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. | The fix is designed to close file descriptors within the truncated part of the parcel. |
| Platform | 12,12L,13,14,15 | CVE-2023-40122 | In applyCustomDescription of SaveUi.java, there is a possible way to view another user's image content. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. | The fix is designed to verify that the user has permission to view the URI. |
| Platform | 12,12L,13,14,15 | CVE-2024-0037 | In renderSuggestion of RemoteInlineSuggestionViewConnector.java , there is a possible way to view images belonging to a different user of the device due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation. | The fix is designed to add the missing URI permission check. |
| Platform | 12,12L,13,14,15 | CVE-2025-0100 | In onCreate of MediaProjectionPermissionActivity.java, there is a possible way to bypass user consent due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. | The fix is designed to ensure the calling package has the appropriate permission. |
| Platform | 12,12L,13,14,15 | CVE-2024-49741 | In multiple functions of AppWidgetServiceImpl.java, there is a possible persistent denial of service due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. | The fix is designed to implement limits on hosts per package and widgets per host. |
| Platform | 12,12L,13,14,15 | CVE-2025-0094 | In onCreateOptionsMenu of UserSettings.java, there is a possible way to remove the work profile by opening a hidden activity due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. | The fix is designed to prevent the User Settings overflow menu from appearing when interacting with a work profile. |
| Platform | 12,12L,13,14,15 | CVE-2023-24023 | In multiple locations, there is a possible way to impersonate and MitM a device across session by only compromising one session key due to an insecure protocol design on Bluetooth Legacy Secure Connection (LSC). This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. | The fix is designed to add support for both checking security downgrade and disallowing connect, when certain downgrades occur. |
| Platform | 12,12L,13,14,15 | CVE-2025-0091 | In isSafeIntent of AccountManagerService.java, there is a possible way to bypass an intent type check due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. | The fix is designed to implement an additional check against unsafe intent types. |
| Platform | 14,15 | CVE-2025-0095 | In AppTimeSpentPresenter of AppTimeSpentPreference.kt, there is a possible way to hijack implicit intent. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. | The fix is designed to set a specific package to its corresponding intent. |
| Platform | 12,12L,13,14,15 | CVE-2024-49729 | In GetTable of dm.cpp, there is a possible way to leak the raw FDE key in bug reports due to improperly used crypto. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. | The fix is designed to redact keys from dm-crypt targets. |
| Platform | 12,12L,13,14 | CVE-2024-0032 | In multiple locations, there is a possible way to request access to directories that should be hidden due to improper input validation. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation. | The fix is designed to restrict access for specific directories and subdirectories in shared storage. |
| Platform | 12,12L,13,14,15 | CVE-2024-43093 | In shouldHideDocument of ExternalStorageProvider.java, there is a possible bypass of a file path filter designed to prevent access to sensitive directories due to incorrect unicode normalization. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. | The fix is designed to restrict access to select directories. |
| Platform | 12,12L,13,14,15 | CVE-2025-0078 | In main of main.cpp, there is a possible way to bypass SELinux due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. | The fix is designed to set the correct flags to become a context object. |
| Platform | 12,12L,13,14,15 | CVE-2025-0087 | In onCreate of UninstallerActivity.java, there is a possible way to uninstall a different user's app due to nothing consequential. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. | The fix is designed to ensure that only the parent profile can uninstall the app that is in the child profiles. |
| Platform | 12,12L,13,14,15 | CVE-2024-43090 | In multiple locations, there is a possible cross-user image read due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation. | The fix is designed to clear any icon that may have been set. |
| Platform | 12,12L,13,14,15 | CVE-2025-0083 | In multiple locations, there is a possible way to access content across user profiles due to URI double encoding. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. | The fix is designed to resolve a cross account user icon validation. |
| Platform | 12,12L,13,14,15 | CVE-2025-0086 | In onResult of AccountManagerService.java, there is a possible way to overwrite auth token due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. | The fix is designed to check the account type. |
| Platform | 12,12L,13,14,15 | CVE-2024-49740 | In multiple locations, there is a possible crash loop due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. | The fix is designed to enforce character size limits. |
| Platform | 13,14,15 | CVE-2025-0084 | In multiple locations, there is a possible out of bounds write due to a use after free. This could lead to remote code execution over Bluetooth, if HFP support is enabled, with no additional execution privileges needed. User interaction is not needed for exploitation. | The fix is designed to check during discovery if a database has already been allocated. |
| Platform | 12,12L,13,14,15 | CVE-2025-0081 | In dng\_lossless\_decoder::HuffDecode of dng\_lossless\_jpeg.cpp, there is a possible way to cause a crash due to uninitialized data. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. | The fix is designed to catch null HuffmanTables when decoding jpeg. |
| Platform | 12,12L,13,14,15 | CVE-2025-0079 | In multiple locations, there is a possible way that avdtp and avctp channels could be unencrypted due to a logic error in the code. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation. | The fix is designed to remove flags for the avdtp and avctp channels. |
| Platform | 12,12L,13,14,15 | CVE-2024-49728 | In generateFileInfo of BluetoothOppSendFileInfo.java, there is a possible cross user media disclosure due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. | The fix is designed to implement an additional validation check against content URIs. |
| Platform | 12,12L,13,14,15 | CVE-2025-0082 | In multiple functions of StatusHint.java and TelecomServiceImpl.java, there is a possible way to reveal images across users due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. | The fix is designed to validate that images belong to the calling user. |
| Platform | 12,12L,13,14,15 | CVE-2025-0092 | In handleBondStateChanged of AdapterService.java, there is a possible permission bypass due to misleading or insufficient UI. This could lead to remote (proximal/adjacent) information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. | The fix is designed to remove permissions when the device is unbonded. |
| Platform | 12,12L,13,14,15 | CVE-2025-0093 | In handleBondStateChanged of AdapterService.java, there is a possible unapproved data access due to a missing permission check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. | The fix is designed to remove permissions when the device is unbonded. |
| Platform | 12,12L,13,14,15 | CVE-2025-26417 | In checkWhetherCallingAppHasAccess of DownloadProvider.java, there is a possible bypass of user consent when opening files in shared storage due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. | The fix is designed to enforce file ownership in the provider. |