INFORME DE ESCANEO DE VULNERABILIDADES VIT

PLAN DE TRABAJO MARZO -MAYO 2025

**Objetivo**

MOSTAR UN RESUMEN GENERAL DE LOS HALLAZGOS ENCONTRADOS TRAS EL EJERCICIO DE ESCANEO DE VULNERABILIDADES REALIZADO, ASI COMO ESTABLECER UN PLAN DE TRABAJO PARA LA REMEDICACION DE LAS VULNERABILIDADES ENCONTRADAS.

**Resumen de Vulnerabilidades:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Plataforma | Crítico | Alto | Medio | Bajo | Informativo | Total |
| Android | 0 | 3 | 7 | 3 | 1 | **14** |
| iOS | 0 | 2 | 4 | 1 | 0 | **7** |

**Detalle de Vulnerabilidades:**

[*Reporte de resultados*](https://vectorcb-my.sharepoint.com/:b:/g/personal/jlozano_vector_com_mx/EeTzoKlbwqpBsiFG3R1vqPgB1-QsRJjivseJ9K0Kyw83OA?e=dav6Hl)

* **Vulnerabilidades Altas:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Severity** | **CVSS v4.0** | **ID** | **Name** |
| **High** | **8.2** | *MOB-AND-HA1* | Falla en la lógica de control del flujo de la aplicación |
| **High** | **7** | *MOB-AND-HA2* | Ausencia de controles para la detección de herramientas de instrumentación |
| **High** | **7** | *MOB-AND-HA3* | Falta de mecanismos de detección de root en la aplicación móvil |
| **High** | **7** | *MOB-IOS-HA01* | Ausencia de controles para la detección de herramientas de instrumentación |
| **High** | **7** | *MOB-IOS-HA02* | Falta de controles en protección anti-jailbreak |

* **Vulnerabilidades Medias:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Severity** | **CVSS v4.0** | **ID** | **Name** |
| **Medium** | **6.9** | *MOB-AND-HA4* | Ausencia de mecanismos de mitigación contra ataques de fuerza bruta en autenticación |
| **Medium** | **6.9** | *MOB-AND-HA5* | Vulnerabilidad de enumeración de usuarios |
| **Medium** | **6.8** | *MOB-AND-HA6* | Proceso de reconocimiento facial susceptible a manipulación |
| **Medium** | **6.3** | *MOB-AND-HA7* | Validación inadecuada en campos de entrada |
| **Medium** | **6** | *MOB-AND-HA8* | Ausencia de protección FORTIFY\_SOURCE en binarios de la aplicación |
| **Medium** | **5.8** | *MOB-AND-HA9* | Información de usuario enrolado almacenado en dispositivo |
| **Medium** | **5.1** | *MOB-AND-HA10* | Ausencia de controles de ofuscación en el código fuente |
| **Medium** | **6** | *MOB-IOS-HA03* | Característica Stack Protection deshabilitada |
| **Medium** | **5.8** | *MOB-IOS-HA04* | Información de usuario enrolado almacenado en dispositivo |
| **Medium** | **5.1** | *MOB-IOS-HA05* | Ausencia de controles de ofuscación en el código fuente |
| **Medium** | **5.8** | *MOB-IOS-HA06* | Contraseñas almacenadas en texto claro en el Keychain de iOS |

* **Vulnerabilidades Bajas:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Severity** | **CVSS v4.0** | **ID** | **Name** |
| **Low** | **2.3** | *MOB-AND-HA11* | Uso de cifrados débiles para la comunicación |
| **Low** | **2.1** | *MOB-AND-HA12* | Código de depuración habilitado en StrictMode |
| **Low** | **2** | *MOB-AND-HA13* | Versión de firmado de aplicación vulnerable |
| **Low** | **2.3** | *MOB-IOS-HA07* | Funciones ATS deshabilitadas |

* **Vulnerabilidades Informativas:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Severity** | **CVSS v4.0** | **ID** | **Name** |
| **Informative** | **0** | *MOB-AND-HA14* | Falta de mecanismos de detección de ejecución en emuladores |

**Plan de Trabajo:**

A blue and white bar with black text

AI-generated content may be incorrect.

\*Incidencias de bajo impacto se trabajarán en el Q3.

**Aceptación de Vulnerabilidades:**

|  |  |  |
| --- | --- | --- |
| **Vulnerabilidad** | **Entorno** | **Comentario** |
| Falla en la lógica de control del flujo de la aplicación | Android |  |
| Ausencia de controles para la detección de herramientas de instrumentación | Android & iOS |  |
| Falta de mecanismos de detección de root en la aplicación móvil | Android |  |
| Falta de controles en protección anti-jailbreak | IOS |  |
| Ausencia de mecanismos de mitigación contra ataques de fuerza bruta en autenticación | Android |  |
| Vulnerabilidad de enumeración de usuarios | Android |  |
| Proceso de reconocimiento facial susceptible a manipulación | Android |  |
| Validación inadecuada en campos de entrada | Android |  |
| Ausencia de protección FORTIFY\_SOURCE en binarios de la aplicación | Android |  |
| Información de usuario enrolado almacenado en dispositivo | Android & iOS |  |
| Ausencia de controles de ofuscación en el código fuente | Android & iOS |  |
| Característica Stack Protection deshabilitada | IOS |  |
| Contraseñas almacenadas en texto claro en el Keychain de iOS | IOS |  |
| Uso de cifrados débiles para la comunicación | Android |  |
| Código de depuración habilitado en StrictMode | Android |  |
| Versión de firmado de aplicación vulnerable | Android |  |
| Funciones ATS deshabilitadas | IOS |  |
| Falta de mecanismos de detección de ejecución en emuladores | IOS |  |

**Validado por,**

**Aziel García Castillo**  
Director de Innovación  
Vector Casa de Bolsa, S.A. de C.V.