| | |
|---|---|
| **Alerta de seguridad cibernética** | 9VSA24-00975-01 |
| **Clase de alerta** | Vulnerabilidad |
| **Tipo de incidente** | Sistema y/o Software Abierto |
| **TLP** | Blanco |
| **Fecha de lanzamiento original** | 13 de febrero de 2024 |
| **Última revisión** | 13 de febrero de 2024 |

**NOTIFICACIÓN:** La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del CSIRT de Gobierno. La información contenida en los informes o comunicados está afecta a actualizaciones.

## Resumen


El CSIRT de Gobierno comparte información de vulnerabilidades parchadas en varios productos por Adobe, parte de sus actualizaciones del Patch Tuesday del 13 de febrero de 2024.


## Vulnerabilidades

CVE-2024-20723
CVE-2024-20740
CVE-2024-20741
CVE-2024-20742
CVE-2024-20743
CVE-2024-20744
CVE-2024-20722
CVE-2024-20724
CVE-2024-20725
CVE-2024-20726
CVE-2024-20727
CVE-2024-20728
CVE-2024-20729
CVE-2024-20730
CVE-2024-20731
CVE-2024-20733
CVE-2024-20734
CVE-2024-20735
CVE-2024-20736
CVE-2024-20747
CVE-2024-20748
CVE-2024-20749
CVE-2024-20719
CVE-2024-20720
CVE-2024-20750
CVE-2024-20716
CVE-2024-20717
CVE-2024-20718
CVE-2024-20738

## Impacto

**Vulnerabilidades de riesgo crítico:**

CVE-2024-20738: Vulnerabilidad de autenticación inapropiada, que hace posible una evasión de medidas de seguridad. CVSS: 9.8.

CVE-2024-20719: Vulnerabilidad de tipo stored XSS que puede llevar a la ejecución remota de código. CVSS: 9.1.

CVE-2024-20720: Vulnerabilidad de tipo Inyección de comandos OS, que puede llevar a la ejecución remota de código. CVSS: 9.1.

## Mitigación

Instalar las respectivas actualizaciones.
https://www.adobe.com/devnet-docs/acrobatetk/tools/ReleaseNotesDC/index.html#continuous-track
https://www.adobe.com/products/substance3d-painter.html
https://www.adobe.com/in/creativecloud/catalog/desktop.html
https://www.adobe.com/products/substance3d-designer.html

## Productos afectados

Acrobat DC.
Acrobat Reader DC.
Acrobat 2020.
Acrobat Reader 2020.
Adobe Commerce 2.4.6-p3 y anteriores
Adobe Commerce 2.4.5-p5 y anteriores
Adobe Commerce 2.4.4-p6 y anteriores
Adobe Commerce 2.4.3-ext-5 y anteriores
Adobe Commerce 2.4.2-ext-5 y anteriores
Adobe Commerce 2.4.1-ext-5 y anteriores
Adobe Commerce 2.4.0-ext-5 y anteriores
Adobe Commerce 2.3.7-p4-ext-5 y anteriores
Magento Open Source 2.4.6-p3 y anteriores
Magento Open Source 2.4.5-p5 y anteriores
Magento Open Source 2.4.4-p6 y anteriores
Adobe Substance 3D Painter 9.1.2.
Adobe FrameMaker Publishing Server versión 2022 Update 1 y anteriores.
Adobe Audition 24.0.3 y anteriores.
Adobe Audition 23.6.2 y anteriores.
Adobe Substance 3D Designer 13.1.0 y anteriores.

## Enlaces

https://helpx.adobe.com/security/products/acrobat/apsb24-07.html
https://helpx.adobe.com/security/products/magento/apsb24-03.html
https://helpx.adobe.com/security/products/substance3d_painter/apsb24-04.html
https://helpx.adobe.com/security/products/framemaker-publishing-server/apsb24-10.html
https://helpx.adobe.com/security/products/substance3d_designer/apsb24-13.html

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.02.13 16:06:13 -03'00'