| | |
|---|---|
| **Alerta de seguridad cibernética** | 9VSA23-00882-01 |
| **Clase de alerta** | Vulnerabilidad |
| **Tipo de incidente** | Sistema y/o Software Abierto |
| **TLP** | Blanco |
| **Fecha de lanzamiento original** | 10 de agosto de 2023 |
| **Última revisión** | 10 de agosto de 2023 |

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 informadas recientemente por Adobe como parte de sus actualizaciones de seguridad para varios de sus productos.


## Vulnerabilidades

CVE-2023-29320
CVE-2023-29299
CVE-2023-29303
CVE-2023-38222
CVE-2023-38223
CVE-2023-38224
CVE-2023-38225
CVE-2023-38226
CVE-2023-38227
CVE-2023-38228
CVE-2023-38229
CVE-2023-38230
CVE-2023-38231
CVE-2023-38232
CVE-2023-38233
CVE-2023-38234
CVE-2023-38235
CVE-2023-38212
CVE-2023-38211
CVE-2023-38236
CVE-2023-38237
CVE-2023-38238
CVE-2023-38239
CVE-2023-38240
CVE-2023-38207
CVE-2023-38208
CVE-2023-38209
CVE-2023-38210

## Impacto

### Vulnerabilidades de riesgo crítico

CVE-2023-38208: Neutralización inapropiada de Special Elements usados en un comando OS (Inyección de comandos OS) en Adobe Commerce y Magento Open Source. CVSS: 9.1.
CVE-2023-29320: Control de acceso inapropiado en Acrobat. CVSS: 8.6.
CVE-2023-38212: Uso de memoria luego de ser liberada en Dimension. CVSS: 7.8.
CVE-2023-38211: Desborde de buffer basado en lotes en Dimension. CVSS: 7.8.
CVE-2023-38222: Uso de memoria luego de ser liberada en Acrobat. CVSS: 7.8.
CVE-2023-38223: Acceso de puntero (“pointer”) no inicializado en Acrobat. CVSS: 7.8.
CVE-2023-38224: Uso de memoria luego de ser liberada en Acrobat. CVSS: 7.8.
CVE-2023-38225: Uso de memoria luego de ser liberada en Acrobat. CVSS: 7.8.
CVE-2023-38226: Acceso de puntero (“pointer”) no inicializado en Acrobat. CVSS: 7.8.

CVE-2023-38227: Uso de memoria luego de ser liberada en Acrobat. CVSS: 7.8.
CVE-2023-38228: Uso de memoria luego de ser liberada en Acrobat. CVSS: 7.8.
CVE-2023-38229: Lectura fuera de límites de la memoria en Acrobat. CVSS: 7.8.
CVE-2023-38230: Uso de memoria luego de ser liberada en Acrobat. CVSS: 7.8.
CVE-2023-38231: Escritura fuera de límites de la memoria en Acrobat. CVSS: 7.8.
CVE-2023-38232: Lectura fuera de límites de la memoria en Acrobat. CVSS: 7.8.
CVE-2023-38233: Escritura fuera de límites de la memoria en Acrobat. CVSS: 7.8.
CVE-2023-38234: Acceso de puntero ("pointer") no inicializado en Acrobat. CVSS: 7.8.
CVE-2023-38235: Lectura fuera de límites de la memoria en Acrobat. CVSS: 7.8.

## Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

## Productos afectados

Adobe XMP-Toolkit-SDK 2022.06 y anteriores.
Adobe Dimension 3.4.9 y anteriores.
Adobe Commerce 2.4.6-p1 y anteriores.
Magento Open Source 2.4.6-p1 y anteriores.
Acrobat DC Continuous 23.003.20244 y anteriores.
Acrobat Reader DC Continuous 23.003.20244 y anteriores.
Acrobat Reader 2020 Classic 2020 23.003.20244 y anteriores.
Acrobat Reader 2020 Classic 2020 20.005.30467 y anteriores.

## Enlaces

https://helpx.adobe.com/security/products/acrobat/apsb23-30.html
https://helpx.adobe.com/security/products/magento/apsb23-42.html
https://helpx.adobe.com/security/products/dimension/apsb23-44.html
https://helpx.adobe.com/security/products/xmpcore/apsb23-45.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29320
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29299
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29303
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38222
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38223
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38224
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38225
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38226
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38227
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38228
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38229
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38230
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38231
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38232
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38233
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38234

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38235
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38212
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38211
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38236
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38237
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38238
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38239
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38240
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38207
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38208
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38209
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38210

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.08.10 14:03:16 -04'00'