Alerta de seguridad cibernética	9VSA23-00849-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	14 de junio de 2023
Última revisión	14 de junio 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 parchadas por Adobe recientemente para varios de sus productos.

Vulnerabilidades

CVE-2023-29304
CVE-2023-29307
CVE-2023-29322
CVE-2023-29302
CVE-2023-29287
CVE-2023-29288
CVE-2023-29289
CVE-2023-29290
CVE-2023-29291
CVE-2023-29292
CVE-2023-29293
CVE-2023-29294
CVE-2023-29295
CVE-2023-29296
CVE-2023-29297
CVE-2023-22248
CVE-2023-29321

Impacto

Vulnerabilidades de riesgo crítico
CVE-2023-29297: Vulnerabilidad de ejecución arbitraria de código. CVSS 9.1.
CVE-2023-22248: Bypass de función de seguridad. CVSS 7.5.
CVE-2023-29321: Vulnerabilidad de ejecución arbitraria de código. CVSS 7.8.
CVE-2023-21618: Vulnerabilidad de acceso a puntero no inicializado. CVSS 7.8.

Mitigación
Instalar las respectivas actualizaciones entregadas por el proveedor.

Productos afectados
Adobe Experience Manager (AEM) 6.5.17.0 y anteriores.

Adobe Commerce 2.4.6 y anteriores, 2.4.5-p2 y anteriores, 2.4.4-p3 y anteriores, 2.4.3-ext-2 y anteriores, 2.4.2-ext-2 y anteriores, 2.4.1-ext-2 y anteriores, 2.4.0-ext-2 y anteriores, 2.3.7-p4-ext-2 y anteriores.
Magento Open Source 2.4.6 y anteriores, 2.4.5-p2 y anteriores, 2.4.4-p3 y anteriores.
Adobe Animate 2022 22.0.9 y anteriores.
Adobe Animate 2023 23.0.1 y anteriores.

Enlaces

https://helpx.adobe.com/security/products/experience-manager/apsb23-31.html
https://helpx.adobe.com/security/products/magento/apsb23-35.html
https://helpx.adobe.com/security/products/animate/apsb23-36.html
https://helpx.adobe.com/security/products/substance3d_designer/apsb23-39.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29304
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29307
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29322
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29302
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29287
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29288
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29289
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29290
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29291
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29292
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29293
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29294
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29295
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29296
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29297
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22248
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29321

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.06.14 17:30:44 -04'00'