

Alerta de seguridad cibernética	9VSA21-00494-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de septiembre de 2021
Última revisión	14 de septiembre de 2021

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 equipo CSIRT. La información contenida en los informes o comunicados está afectada a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, CSIRT de Gobierno, comparte información relacionada con múltiples vulnerabilidades divulgadas por Adobe y que afectan a varios de sus productos.

Este informe incluye las medidas de mitigación, consistentes en instalar la última actualización de los productos afectados.

Vulnerabilidades

CVE-2021-28613	CVE-2021-39835	CVE-2021-39855
CVE-2021-35982	CVE-2021-39836	CVE-2021-39856
CVE-2021-39818	CVE-2021-39837	CVE-2021-39857
CVE-2021-39819	CVE-2021-39838	CVE-2021-39858
CVE-2021-39820	CVE-2021-39839	CVE-2021-39859
CVE-2021-39821	CVE-2021-39840	CVE-2021-39860
CVE-2021-39822	CVE-2021-39841	CVE-2021-39861
CVE-2021-39823	CVE-2021-39842	CVE-2021-39863
CVE-2021-39824	CVE-2021-39843	CVE-2021-40698
CVE-2021-39825	CVE-2021-39844	CVE-2021-40699
CVE-2021-39826	CVE-2021-39845	CVE-2021-40700
CVE-2021-39827	CVE-2021-39846	CVE-2021-40701
CVE-2021-39828	CVE-2021-39849	CVE-2021-40702
CVE-2021-39831	CVE-2021-39850	CVE-2021-40703
CVE-2021-39830	CVE-2021-39851	CVE-2021-40708
CVE-2021-39832	CVE-2021-39852	CVE-2021-40709
CVE-2021-39833	CVE-2021-39853	CVE-2021-40710
CVE-2021-39834	CVE-2021-39854	CVE-2021-40711

CVE-2021-40712
CVE-2021-40713
CVE-2021-40714
CVE-2021-40715

CVE-2021-40716
CVE-2021-40697

Impactos

Consideradas críticas por Adobe:

CVE-2021-39818: Ejecución arbitraria de código en Adobe InCopy.
CVE-2021-39819: Escritura arbitraria de archivos en Adobe InCopy.
CVE-2021-39820: Ejecución arbitraria de código en Adobe InDesign.
CVE-2021-39821: Ejecución arbitraria de código en Adobe InDesign.
CVE-2021-39822: Ejecución arbitraria de código en Adobe InDesign.
CVE-2021-39823: Ejecución arbitraria de código en Adobe SVG-Native-Viewer.
CVE-2021-39826: Ejecución arbitraria de código en Adobe Digital Editions.
CVE-2021-39827: Escritura arbitraria de archivos en Adobe Digital Editions.
CVE-2021-39830: Ejecución arbitraria de código en Framemaker.
CVE-2021-39836: Ejecución arbitraria de código en Adobe Acrobat y Reader.
CVE-2021-39852: Denegación de servicio en Adobe Acrobat y Reader.
CVE-2021-39837: Ejecución arbitraria de código en Adobe Acrobat y Reader.
CVE-2021-39838: Ejecución arbitraria de código en Adobe Acrobat y Reader.
CVE-2021-39839: Ejecución arbitraria de código en Adobe Acrobat y Reader.
CVE-2021-39840: Ejecución arbitraria de código en Adobe Acrobat y Reader.
CVE-2021-39841: Ejecución arbitraria de código en Adobe Acrobat y Reader.
CVE-2021-39843: Fuga de memoria en Adobe Acrobat y Reader.
CVE-2021-39844: Fuga de memoria en Adobe Acrobat y Reader.
CVE-2021-39845: Ejecución arbitraria de código en Adobe Acrobat y Reader.
CVE-2021-39846: Ejecución arbitraria de código en Adobe Acrobat y Reader.
CVE-2021-39863: Ejecución arbitraria de código en Adobe Acrobat y Reader.
CVE-2021-40708: Escalamiento de privilegios en Adobe Genuine Service.
CVE-2021-40709: Ejecución arbitraria de código en Adobe Photoshop.
CVE-2021-40710: Ejecución arbitraria de código en Adobe Premiere Pro.
CVE-2021-40711: Ejecución arbitraria de código en Adobe Experience Manager (AEM).
CVE-2021-40715: Ejecución arbitraria de código en Adobe Premiere Pro.
CVE-2021-40698: Evasión de la función de seguridad en ColdFusion.
CVE-2021-40699: Evasión de la función de seguridad ColdFusion.

Productos Afectados

Adobe Premiere Elements
Adobe Premiere Pro
Adobe Genuine Integrity Service
Adobe SVG-Native-Viewer
Adobe XMP-Toolkit-SDK
Adobe Photoshop

Adobe Photoshop Elements
Adobe InCopy
Adobe InDesign
Adobe Experience Manager (AEM)
Adobe Creative Cloud Desktop Application
Adobe ColdFusion
Adobe Acrobat and Reader

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

<https://helpx.adobe.com/security/products/acrobat/apsb21-55.html>
https://helpx.adobe.com/security/products/premiere_pro/apsb21-67.html
<https://helpx.adobe.com/security/products/incopy/apsb21-71.html>
<https://helpx.adobe.com/security/products/indesign/apsb21-73.html>
<https://helpx.adobe.com/security/products/coldfusion/apsb21-75.html>
<https://helpx.adobe.com/security/products/creative-cloud/apsb21-76.html>
https://helpx.adobe.com/security/products/photoshop_elements/apsb21-77.html
https://helpx.adobe.com/security/products/premiere_elements/apsb21-78.html
<https://helpx.adobe.com/security/products/Digital-Editions/apsb21-80.html>
https://helpx.adobe.com/security/products/integrity_service/apsb21-81.html
<https://helpx.adobe.com/security/products/experience-manager/apsb21-82.html>
<https://helpx.adobe.com/security/products/photoshop/apsb21-84.html>
<https://helpx.adobe.com/security/products/xmpcore/apsb21-85.html>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35982>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39818>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39819>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39820>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39821>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39822>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39823>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39824>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39825>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39826>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39827>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39828>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39831>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39830>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39832>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39833>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39834>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39835>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39836>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39837>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39838>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39839>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39840>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39841>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39842>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39843>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39844>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39845>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39846>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39849>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39850>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39850>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39852>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39853>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39854>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39855>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39856>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39857>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39858>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39859>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39860>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39861>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39863>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40698>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40699>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40700>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40701>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40702>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40703>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40708>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40709>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40710>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40711>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40712>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40713>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40714>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40715>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40716>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40697>