Alerta de seguridad cibernética	9VSA21-00513-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	27 de octubre de 2021
Última revisión	27 de octubre 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 afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, CSIRT de Gobierno, comparte información sobre nuevas vulnerabilidades en productos de Adobe.

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

Vulnerabilidades

CVE-2021-40718	CVE-2021-40787	CVE-2021-42267	CVE-2021-42528
CVE-2021-40733	CVE-2021-40788	CVE-2021-42268	CVE-2021-42529
CVE-2021-40743	CVE-2021-40789	CVE-2021-42269	CVE-2021-42530
CVE-2021-40746	CVE-2021-40792	CVE-2021-42270	CVE-2021-42531
CVE-2021-40747	CVE-2021-40793	CVE-2021-42271	CVE-2021-42532
CVE-2021-40748	CVE-2021-40794	CVE-2021-42272	CVE-2021-42731
CVE-2021-40749	CVE-2021-40796	CVE-2021-42524	CVE-2021-42732
CVE-2021-40776	CVE-2021-42263	CVE-2021-42525	CVE-2021-42734
CVE-2021-40785	CVE-2021-42264	CVE-2021-42526	CVE-2021-42735
CVE-2021-40786	CVE-2021-42266	CVE-2021-42527	CVE-2021-42736

Impactos

Riesgo alto:

CVE-2021-40718: La vulnerabilidad existe debido a un error de límites de memoria, que permite a un atacante remoto ejecutar código arbitrario al desatar corrupción de memoria.

CVE-2021-40733: La vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en el sistema, debido a un error de límites de la memoria al procesar input no confiable, a través de lo cual un atacante remoto puede detonar corrupción de memoria y ejecutar código arbitrario en el sistema objetivo.

CVE-2021-40746: La vulnerabilidad existe debido a un error de límites de memoria, que permite a un atacante remoto ejecutar código arbitrario al desatar corrupción de memoria.

CVE-2021-40776: La vulnerabilidad existe debido a la creación de un archivo temporal en directorio con permisos incorrectos, que lleva a un bypass de restricciones de seguridad y permite a un atacante remoto escalar privilegios en un sistema vulnerable.

CVE-2021-40786: La vulnerabilidad existe debido a un error de límites de memoria, que permite a un atacante remoto ejecutar código arbitrario al desatar corrupción de memoria.

CVE-2021-40787: La vulnerabilidad existe debido a un error de límites de memoria, que permite a un atacante remoto ejecutar código arbitrario al desatar corrupción de memoria.

CVE-2021-40792: La vulnerabilidad existe debido a un error de límites de memoria, que permite a un atacante remoto ejecutar código arbitrario al desatar corrupción de memoria.

CVE-2021-42524: La vulnerabilidad existe debido a un error de límites de memoria, que permite a un atacante remoto ejecutar código arbitrario al desatar corrupción de memoria.

CVE-2021-42529: La vulnerabilidad existe debido a un error de límites de memoria, que permite a un atacante remoto ejecutar código arbitrario al desatar corrupción de memoria.

CVE-2021-42530: La vulnerabilidad existe debido a un error de límites de memoria, que permite a un atacante remoto ejecutar código arbitrario al desatar corrupción de memoria.

CVE-2021-42531: La vulnerabilidad existe debido a un error de límites de memoria, que permite a un atacante remoto ejecutar código arbitrario al desatar corrupción de memoria.

CVE-2021-42532: La vulnerabilidad existe debido a un error de límites de memoria, que permite a un atacante remoto ejecutar código arbitrario al desatar corrupción de memoria.

CVE-2021-42266: La vulnerabilidad existe debido a un error de límites de memoria, que permite a un atacante remoto ejecutar código arbitrario al desatar corrupción de memoria.

CVE-2021-42267: La vulnerabilidad existe debido a un error de límites de memoria, que permite a un atacante remoto ejecutar código arbitrario al desatar corrupción de memoria.

CVE-2021-42268: La vulnerabilidad existe debido a un error NULL pointer dereference, que permite a un atacante remoto ejecutar código arbitrario al desatar corrupción de memoria.

CVE-2021-42269: La vulnerabilidad existe debido a un error de uso de memoria después de ser liberada, que permite a un atacante remoto ejecutar código arbitrario al desatar corrupción de memoria.

CVE-2021-42270: La vulnerabilidad existe debido a un error de límites de memoria, que permite a un atacante remoto ejecutar código arbitrario al desatar corrupción de memoria.

CVE-2021-42271: La vulnerabilidad existe debido a un error de límites de memoria, que permite a un atacante remoto ejecutar código arbitrario al desatar corrupción de memoria.

CVE-2021-42272: La vulnerabilidad existe debido a un error de límites de memoria, que permite a un atacante remoto ejecutar código arbitrario al desatar corrupción de memoria.

CVE-2021-42526: La vulnerabilidad existe debido a un error de límites de memoria, que permite a un atacante remoto ejecutar código arbitrario al desatar corrupción de memoria.

CVE-2021-42527: La vulnerabilidad existe debido a un error de límites de memoria, que permite a un atacante remoto ejecutar código arbitrario al desatar corrupción de memoria.

CVE-2021-42731: La vulnerabilidad existe debido a un error de límites de memoria, que permite a un atacante remoto ejecutar código arbitrario al desatar corrupción de memoria.

CVE-2021-42732: La vulnerabilidad existe debido a un error de límites de memoria, que permite a un atacante remoto ejecutar código arbitrario al desatar corrupción de memoria.

CVE-2021-42735: La vulnerabilidad existe debido a un error de límites de memoria al procesar archivos de Photoshop, que permite a un atacante remoto enviar un archivo especialmente diseñado a la víctima, desatar corrupción de memoria y ejecutar código arbitrario en el sistema objetivo.

CVE-2021-42736: La vulnerabilidad existe debido a un error de límites de memoria al procesar archivos de Photoshop, que permite a un atacante remoto enviar un archivo especialmente diseñado a la víctima, desatar corrupción de memoria y ejecutar código arbitrario en el sistema objetivo.

Productos Afectados

Adobe Illustrator CC: 25.0 a 25.4.1.
Adobe Premiere Elements: 2021.19.0 20210809.daily.2242976.
Adobe InDesign: 9.1.0 a 2015.
Adobe Lightroom Classic: 10.3
Adobe Animate 21.0.9.
Adobe Photoshop: 20.0 a 22.5.1.
Adobe Premiere Pro 13.1.0 a 15.4.1.
Adobe Premiere Elements: 2021.19.0 20210809.daily.2242976
Adobe InDesign: 9.1.0 a 2014.2, 2015.
Adobe Lightroom Classic 10.3.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

http://helpx.adobe.com/security/products/illustrator/apsb21-98.html
http://helpx.adobe.com/security/products/premiere_elements/apsb21-106.html
http://helpx.adobe.com/security/products/indesign/apsb21-107.html
http://helpx.adobe.com/security/products/lightroom/apsb21-97.html
http://helpx.adobe.com/security/products/animate/apsb21-105.html
http://helpx.adobe.com/security/products/photoshop/apsb21-109.html
http://helpx.adobe.com/security/products/premiere_pro/apsb21-100.html
http://helpx.adobe.com/security/products/xmpcore/apsb21-108.html
http://helpx.adobe.com/security/products/premiere_elements/apsb21-106.html

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.10.28 10:53:18 -03'00'