Alerta de seguridad cibernética	9VSA21-00466-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de julio de 2021
Última revisión	14 de julio 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 vulnerabilidades que afectan a diversos productos de Adobe.

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

Vulnerabilidades

CVE-2021-35981
CVE-2021-35983
CVE-2021-35984
CVE-2021-35985
CVE-2021-35986
CVE-2021-35987
CVE-2021-35988
CVE-2021-35989
CVE-2021-35990
CVE-2021-35991
CVE-2021-35992
CVE-2021-35980
CVE-2021-28624
CVE-2021-28634
CVE-2021-28635
CVE-2021-28636
CVE-2021-28637
CVE-2021-28638
CVE-2021-28639
CVE-2021-28640
CVE-2021-28641
CVE-2021-28642
CVE-2021-28643
CVE-2021-28644
CVE-2021-28591
CVE-2021-28592
CVE-2021-28593
CVE-2021-28595
CVE-2021-28596

Impactos

Adobe considera como vulnerabilidades críticas las siguientes:

CVE-2021-35980 y CVE-2021-28644 afectan a Acrobat Reader y permiten la lectura arbitraria del sistema de archivos.

CVE-2021-28639, CVE-2021-28640 y CVE-2021-28641, son errores de uso de memoria luego de ser liberada que afectan a Acrobat Reader y permiten ejecución arbitraria de código.

CVE-2021-28642 es un error de escritura fuera de los límites de memoria que afecta a Acrobat Reader y permite escritura arbitraria en el sistema de archivos.

CVE-2021-28643 es un error de confusión de tipo de archivo que afecta a Acrobat Reader y permite ejecución arbitraria de código.

CVE-2021-28634 afecta a Acrobat Reader y permite inyección de comandos OS.

CVE-2021-28635, CVE-2021-35981 y CVE-2021-35983 son errores de uso de memoria después de ser liberada en Acrobat Reader que permiten ejecución remota de código.

CVE-2021-28636 afecta a Acrobat Reader y permite ejecución arbitraria de código.

CVE-2021-28637 es un error de lectura fuera de los límites de memoria que afecta a Acrobat Reader y permite fuga de memoria.

CVE-2021-28638 es un error de desborde de buffer en Acrobat Reader que permite ejecución arbitraria de código.

CVE-2021-28595: Afecta a Dimension y posibilita la ejecución arbitraria de código.

CVE-2021-28591 y CVE-2021-28592: Afectan a Illustrator 2021. Son errores de escritura fuera de los límites de la memoria que permiten ejecución arbitraria de código.

CVE-2021-28596: Afecta a Framemaker. Es un error de escritura fuera de los límites de la memoria que permite ejecución arbitraria de código.

CVE-2021-28624, CVE-2021-35989, CVE-2021-35990 y CVE-2021-35991 afectan a Bridge y permiten ejecución arbitraria de código.

Productos Afectados

Adobe Dimension 3.4 y anteriores
Adobe Illustrator 2021 25.2.3 y anteriores.
Adobe Framemaker 2019 Release Update 8 (hotfix) y 2020 Release Update 2.
Adobe Acrobat DC y Reader DC 2021.005.20054 y anteriores.
Adobe Acrobat 2020 y Acrobat Reader 2020 2020.004.30005 y anteriores
Adobe Acrobat 2017 y Acrobat Reader 2017, 2017.011.30197 y anteriores.
Adobe Bridge 11.0.2 y anteriores.

Mitigación

Instalar las respectivas actualizaciones desde el sitio web del proveedor.

Enlaces

https://helpx.adobe.com/security.html
https://helpx.adobe.com/security/products/dimension/apsb21-40.html
https://helpx.adobe.com/security/products/illustrator/apsb21-42.html
https://helpx.adobe.com/security/products/framemaker/apsb21-45.html
https://helpx.adobe.com/security/products/acrobat/apsb21-51.html
https://helpx.adobe.com/security/products/bridge/apsb21-53.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35981
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35983
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35984
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35985
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35986
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35987
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35988
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35989
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35990
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35991
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35992
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35980
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28624
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28634
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28635
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28636
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28637
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28638
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28639
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28640
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28641
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28642
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28643
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28644
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28591
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28592
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28593
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28595
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28596

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.07.14 19:54:31 -04'00'