Alerta de seguridad cibernética	9VSA22-00635-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	11 de mayo de 2022
Última revisión	11 de mayo de 2022

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 Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT de Gobierno, comparte la información que comparte la información de nuevas vulnerabilidades entregada por Adobe para varios de sus productos.

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

Vulnerabilidades

CVE-2022-28818	CVE-2022-28825	CVE-2022-28831
CVE-2022-28819	CVE-2022-28826	CVE-2022-28832
CVE-2022-28821	CVE-2022-28827	CVE-2022-28833
CVE-2022-28822	CVE-2022-28828	CVE-2022-28834
CVE-2022-28823	CVE-2022-28829	CVE-2022-28835
CVE-2022-28824	CVE-2022-28830	CVE-2022-28836

Impacto

Vulnerabilidades críticas

CVE-2022-28819: Vulnerabilidad crítica de ejecución remota de código debido a un error de escritura fuera de los límites de la memoria en Adobe Character Animator.

CVE-2022-28821: Vulnerabilidad crítica de ejecución remota de código debido a un error de escritura fuera de los límites de la memoria en Framemarker.

CVE-2022-28822: Vulnerabilidad crítica de ejecución remota de código debido a un error de escritura fuera de los límites de la memoria en Framemaker.

CVE-2022-28823: Vulnerabilidad crítica de ejecución remota de código debido a un error de uso de memoria luego de ser liberada en Framemaker.

CVE-2022-28824: Vulnerabilidad crítica de ejecución remota de código debido a un error de uso de memoria luego de ser liberada en Framemaker.

CVE-2022-28825: Vulnerabilidad crítica de ejecución remota de código debido a un error de escritura fuera de los límites de la memoria en Framemaker.

CVE-2022-28826: Vulnerabilidad crítica de ejecución remota de código debido a un error de escritura fuera de los límites de la memoria en Framemaker.

CVE-2022-28827: Vulnerabilidad crítica de ejecución remota de código debido a un error de escritura fuera de los límites de la memoria en Framemaker.

CVE-2022-28828: Vulnerabilidad crítica de ejecución remota de código debido a un error de escritura fuera de los límites de la memoria en Framemaker.

CVE-2022-28829: Vulnerabilidad crítica de ejecución remota de código debido a un error de escritura fuera de los límites de la memoria en Framemaker.

CVE-2022-28831: Vulnerabilidad crítica de ejecución remota de código debido a un error de escritura fuera de los límites de la memoria en Adobe InDesign.

CVE-2022-28832: Vulnerabilidad crítica de ejecución remota de código debido a un error de lectura fuera de los límites de la memoria en Adobe InDesign.

CVE-2022-28833: Vulnerabilidad crítica de ejecución remota de código debido a un error de escritura fuera de los límites de la memoria en Adobe InDesign.

CVE-2022-28834: Vulnerabilidad crítica de ejecución remota de código debido a un error de escritura fuera de los límites de la memoria en Adobe InCopy.

CVE-2022-28835: Vulnerabilidad crítica de ejecución remota de código debido a un error uso de memoria luego de ser liberada en Adobe InCopy.

CVE-2022-28836: Vulnerabilidad crítica de ejecución remota de código debido a un error de escritura fuera de los límites de la memoria en Adobe InCopy.

Productos afectados

Character Animator 2021 4.4.2 y anteriores.
Character Animator 2022 22.3 y anteriores.

ColdFusion 2018 Update 13 y anteriores.
ColdFusion 2021 Version 3 y anteriores.
Adobe InDesign 17.1 y anteriores.
Adobe InDesign 16.4.1 y anteriores.
Adobe Framemaker 2019 Update 8 y anteriores.
Adobe Framemaker 2020 Update 4 y anteriores.
Adobe InCopy 17.1 y anteriores.
Adobe InCopy 16.4.1 y anteriores.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://helpx.adobe.com/security/products/character_animator/apsb22-21.html
https://helpx.adobe.com/security/products/coldfusion/apsb22-22.html
https://helpx.adobe.com/security/products/indesign/apsb22-23.html
https://helpx.adobe.com/security/products/framemaker/apsb22-27.html
https://helpx.adobe.com/security/products/incopy/apsb22-28.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28818
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28819
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28821
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28822
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28823
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28824
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28825
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28826
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28827
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28828
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28829
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28830
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28831
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28832
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28833
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28834
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28835
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28836