Alerta de seguridad cibernética	9VSA20-00251-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de junio de 2020
Última revisión	24 de junio de 2020

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, CSIRT, comparte la información obtenida de Adobe referente a tres vulnerabilidades que afectan a su procesador de documentos Adobe FrameMaker. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidades

CVE-2020-9636
CVE-2020-9634
CVE-2020-9635

Vulnerabilidades

CVE-2020-9636: Es posible para un atacante corromper la memoria y realizar un ataque de ejecución de código arbitrario en el sistema afectado.
Impacto: crítico.

CVE-2020-9634, CVE-2020-9635: Un atacante podría escribir fuera de los límites dispuestos en memoria logrando la ejecución de código arbitrario.
Impacto: crítico.

Productos Afectados

Adobe FrameMaker versión 2019.0.5 y anteriores para Windows.

Mitigación

Actualizar a la versión 2019.0.6 de Adobe FrameMaker

Enlaces

https://helpx.adobe.com/security/products/framemaker/apsb20-32.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9636
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9634
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9635