Alerta de seguridad cibernética	9VSA20-00245-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de junio de 2020
Última revisión	15 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 múltiples vulnerabilidades que afectan a sus productos. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidades

CVE-2020-9633
CVE-2020-9634
CVE-2020-9635
CVE-2020-9636
CVE-2020-9643
CVE-2020-9644
CVE-2020-9645
CVE-2020-9647
CVE-2020-9648
CVE-2020-9651

APSB20-30

CVE-2020-9633: Se ha encontrado un error de uso de memoria luego de ser liberada que permitiría a un atacante realizar la ejecución de código arbitrario en el sistema afectado.
Impacto: Crítico.

Productos Afectados

Flash Player para Escritorio versión 32.0.0.371 y anteriores en Windows, macOS y Linux.
Flash Player para Google Chrome versión 32.0.0.371 y anteriores en Windows, macOS, Linux y Chrome OS.
Flash Player para Microsoft Edge e Internet Explorer 11 versión 32.0.0.330 y anteriores en Windows 10 y 8.1.

Mitigación

Para todos los productos, actualizar a la versión 32.0.0.387.
Los enlaces de descarga se encuentran en la página oficial de Adobe.

Enlaces

https://helpx.adobe.com/security/products/flash-player/apsb20-30.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9633

APSB20-31

CVE-2020-9643: Debido a la insuficiente validación de datos ingresados por el usuario, un atacante remoto podría explotar la vulnerabilidad de tipo Server-side request forgery (SSRF), permitiéndole obtener información sensible de la red del sistema afectado, o realizar acciones desde el sistema afectado hacia otros sistemas de la red local.
Impacto: Importante.

CVE-2020-9644: Debido a la insuficiente validación de datos ingresados por el usuario en el explorador, es posible para un atacante realizar un ataque Cross-site Scripting almacenado (Stored XSS), lo que le permitiría realizar la ejecución de código JavaScript en el explorador en el contexto vulnerable.
Impacto: Importante.

CVE-2020-9645: Debido a la insuficiente validación de datos ingresados por el usuario, un atacante remoto podría explotar la vulnerabilidad de tipo Blind Server-side request forgery (SSRF), permitiéndole obtener información sensible de la red del sistema afectado, o realizar acciones desde el sistema afectado hacia otros sistemas de la red local.
Impacto: Importante.

CVE-2020-9647: Debido a la insuficiente validación de datos ingresados por el usuario en el explorador, es posible para un atacante realizar un ataque Cross-site Scripting basado en DOM (DOM-Based XSS), lo que le permitiría realizar la ejecución de código JavaScript en el explorador en el contexto vulnerable.
Impacto: Importante.

CVE-2020-9648: Debido a la insuficiente validación de datos ingresados por el usuario en el explorador, es posible para un atacante realizar un ataque Cross-site Scripting (XSS), lo que le permitiría realizar la ejecución de código JavaScript en el explorador en el contexto vulnerable.
Impacto: Importante.

CVE-2020-9651: Debido a la insuficiente validación de datos ingresados por el usuario en el explorador, es posible para un atacante realizar un ataque Cross-site Scripting reflejado (Reflected XSS), lo que le permitiría realizar la ejecución de código JavaScript en el explorador en el contexto vulnerable.
Impacto: Importante.

Productos Afectados
Adobe Experience Manager versión 6.5 y anteriores.

Mitigación
Aplicar el parche publicado por Adobe su pagina oficial.

Enlaces
https://helpx.adobe.com/security/products/experience-manager/apsb20-31.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9643
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9644
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9645
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9647
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9648
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9651

APSB20-32

CVE-2020-9634, CVE-2020-9635: Se ha encontrado un error de escritura fuera de los límites de la memoria que permitiría a un atacante realizar la ejecución de código arbitrario en el sistema afectado.
Impacto: Crítico.

CVE-2020-9636: Se ha encontrado un error de corrupción en memoria que permitiría a un atacante realizar la ejecución de código arbitrario en el sistema afectado.
Impacto: Crítico.

Productos Afectados

Adobe Framemaker versión 2019.0.5 y anteriores para Windows.

Mitigación

Actualizar Adobe Framemaker a la versión 2019.0.6, disponible en página oficial de Adobe.

Enlaces

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