BAFING

Fecha:		**15/08/2024**	
Detalle reportado:		**Boletín – Vulnerabilidades en productos Adobe**	
Caso de uso:		**CUS_GRL_04_Boletines**	
Severidad:	⚠	Riesgo grave, requiere atención de alta prioridad.	**X**
	⚠	Riesgo intermedio, validación de problemas menores.	
	⚠	No hay problemas graves. Alerta informativa.	
Estado:		**Alertado**	

Descripción

Boletín – Vulnerabilidades en productos Adobe

ADOBE ILLUSTRATOR:

CVE-2024-34133: Vulnerabilidad en Adobe Illustrator permite ejecución de código arbitrario**. - (ALTA)**

Se detectó una vulnerabilidad en Adobe Illustrator debido a una escritura fuera de límite, el cual puede ser aprovechado por un atacante para ejecutar código arbitrario. Al atacante requiere que la víctima interactúe con un archivo malicioso para explotar la vulnerabilidad.

CVE-2024-34118: Vulnerabilidad en Adobe Illustrator permite denegación de servicio**. - (MEDIA)**

Adobe Illustrator cuenta con una vulnerabilidad de validación de entrada incorrecta, el cual permite que un atacante genere una condición de denegación de servicio, al lograr que una víctima abra un archivo malicioso.

Versiones afectadas:

- Adobe Illustrator 2024 versión 28.5 y anteriores
- Adobe Illustrator 2023 versión 27.9.4 y anteriores

Recomendación:

Se recomienda validar si la organización cuenta con las versiones vulnerables de Adobe Illustrator. De ser el caso, aplicar los parches correspondientes para solucionar estas vulnerabilidades.

URL asociado:

- https://helpx.adobe.com/security/products/illustrator/apsb24-45.html

ADOBE DIMENSION:

CVE-2024-34124: Vulnerabilidad en Adobe Dimension permite ejecución de código arbitrario**. - (ALTA)**

Una vulnerabilidad de escritura fuera de límites en Adobe Dimension puede ser aprovechada por un atacante para ejecutar código arbitrario, tras engañar a la víctima para que interactúe con un archivo malicioso.

CVE-2024-41865: Vulnerabilidad en Adobe Dimension permite ejecución de código arbitrario**. - (ALTA)**

Adobe Dimension presenta una vulnerabilidad de ruta de búsqueda no confiable, el cual permite que un atacante pueda ejecutar código arbitrario, al insertar un archivo malicioso en la ruta de búsqueda para que la aplicación ejecute el código cuando localiza ejecutables o bibliotecas.

Versiones afectadas:

- Adobe Dimension versión 3.4.11 y anteriores

Recomendación:
Se recomienda validar si la organización cuenta con las versiones vulnerables de Adobe Dimension. De ser el caso, aplicar los parches correspondientes para solucionar estas vulnerabilidades.

URL asociado:

- https://helpx.adobe.com/security/products/dimension/apsb24-47.html

ADOBE PHOTOSHOP:

CVE-2024-34117: Vulnerabilidad en Adobe Photoshop permite ejecución de código arbitrario**. - (ALTA)**

Se detectó una vulnerabilidad de uso después de la liberación de la memoria en Adobe Photoshop, en la cual un atacante, tras engañar a la víctima para abrir un archivo malicioso, puede ejecutar código arbitrario en el contexto del usuario actual.

Versiones afectadas:

- Adobe Photoshop 2023 versión 24.7.3 y anteriores
- Adobe Photoshop 2024 versión 25.9.1 y anteriores

Recomendación:
Se recomienda validar si la organización cuenta con las versiones vulnerables de Adobe Photoshop. De ser el caso, aplicar los parches correspondientes para solucionar esta vulnerabilidad.

URL asociado:

- https://helpx.adobe.com/security/products/photoshop/apsb24-49.html

ADOBE INDESIGN:

CVE-2024-39389: Vulnerabilidad en Adobe InDesign permite ejecución de código arbitrario**. - (ALTA)**

Una vulnerabilidad de desbordamiento de búfer basada en pila en Adobe InDesign permite que un atacante pueda ejecutar código arbitrario, luego de que una víctima abra un archivo malicioso.

CVE-2024-39390: Vulnerabilidad en Adobe InDesign permite ejecución de código arbitrario**. - (ALTA)**

Un atacante puede aprovechar una vulnerabilidad de escritura fuera de los límites en Adobe InDesign para ejecutar código arbitrario, tras engañar a una víctima para que abra un archivo específicamente diseñado.

Versiones afectadas:

- Adobe InDesign versión ID19.4 y anteriores
- Adobe InDesign versión ID18.5.2 y anteriores

Recomendación:

Se recomienda validar si la organización cuenta con las versiones vulnerables de Adobe InDesign. De ser el caso, aplicar los parches correspondientes para solucionar estas vulnerabilidades.

URL asociado:

- https://helpx.adobe.com/security/products/indesign/apsb24-56.html

ADOBE ACROBAT AND READER:

CVE-2024-39422: Vulnerabilidad en Adobe Acrobat and Reader permite ejecución de código arbitrario**. - (ALTA)**

Se detectó una vulnerabilidad de uso después de liberación de la memoria en Adobe Acrobat and Reader, la cual puede ser aprovechada por un atacante para ejecutar código arbitrario, luego de que la víctima abra un archivo malicioso.

CVE-2024-39425: Vulnerabilidad en Adobe Acrobat and Reader permite elevación de privilegios**. - (ALTA)**

Adobe Acrobat and Reader cuenta con una vulnerabilidad de verificación incorrecta de firma criptográfica de los datos, la cual podría permitir que un atacante, que tenga acceso local con pocos privilegios al sistema vulnerable, pueda escalar sus privilegios.

Versiones afectadas:

- Adobe Acrobat DC y Reader versión 24.002.20991 y anteriores (Windows)
- Adobe Acrobat DC y Reader versión 24.002.20964 y anteriores (macOS)
- Adobe Acrobat 2024 versión 24.001.30123 y anteriores

- Adobe Acrobat 2020 y Acrobat Reader 2020 versión 20.005.30636 y anteriores (Windows)
- Adobe Acrobat 2020 y Acrobat Reader 2020 versión 20.005.30635 y anteriores (macOS)

Recomendación:
Se recomienda validar si la organización cuenta con las versiones vulnerables de Adobe Acrobat and Reader. De ser el caso, aplicar los parches correspondientes para solucionar estas vulnerabilidades.

URL asociado:
- https://helpx.adobe.com/security/products/acrobat/apsb24-57.html

ADOBE BRIDGE:

CVE-2024-39386: Vulnerabilidad en Adobe Bridge permite ejecución de código arbitrario**. - (ALTA)**

Una vulnerabilidad de escritura fuera de los límites en Adobe Bridge permite que un atacante pueda ejecutar código arbitrario, luego de engañar a la víctima para interactuar con un archivo especialmente diseñado.

Versiones afectadas:
- Adobe Bridge versión 13.0.8 y anteriores
- Adobe Bridge versión 14.1.1 y anteriores

Recomendación:
Se recomienda validar si la organización cuenta con las versiones vulnerables de Adobe Bridge. De ser el caso, aplicar los parches correspondientes para solucionar esta vulnerabilidad.

URL asociado:
- https://helpx.adobe.com/security/products/bridge/apsb24-59.html

ADOBE SUBSTANCE 3D STAGER:

CVE-2024-39388: Vulnerabilidad en Adobe Substance 3D Stager permite ejecución de código arbitrario**. - (ALTA)**

Se detectó una vulnerabilidad de uso después de liberación de la memoria en Adobe Substance 3D Stager, en la cual un atacante, tras engañar a la víctima para abrir un archivo malicioso, puede ejecutar código arbitrario en el programa vulnerable.

Versiones afectadas:
- Adobe Substance 3D Stager versión 3.0.2 y anteriores

Recomendación:
Se recomienda validar si la organización cuenta con las versiones vulnerables de Adobe Substance 3D Stager. De ser el caso, aplicar los parches correspondientes para solucionar esta vulnerabilidad.

URL asociado:

- https://helpx.adobe.com/security/products/substance3d_stager/apsb24-60.html

ADOBE COMMERCE:

CVE-2024-39397: Vulnerabilidad en Adobe Commerce permite ejecución de código arbitrario**. - (ALTA)**

Adobe Commerce cuenta con una vulnerabilidad de carga sin restricciones de archivos de tipo peligroso, el cual puede ser aprovechado por un atacante para ejecutar código arbitrario, tras cargar un archivo malicioso que posteriormente se ejecuta en el servidor afectado. No se requiere interacción de la víctima para explotar la vulnerabilidad, pero la complejidad del ataque es alta.

CVE-2024-39398: Vulnerabilidad en Adobe Commerce permite evitar funciones de seguridad**. - (ALTA)**

Una vulnerabilidad de restricción inadecuada de intentos excesivos de autenticación en Adobe Commerce permite que un atacante pueda eludir las funciones de seguridad y generar ataques de fuerza bruta, lo cual puede ocasionar que el atacante obtenga acceso no autorizado al sistema afectado.

Versiones afectadas:

- Adobe Commerce y Adobe Magento Open Source versión 2.4.7-p1 y anteriores
- Adobe Commerce y Adobe Magento Open Source versión 2.4.6-p6 y anteriores
- Adobe Commerce y Adobe Magento Open Source versión 2.4.5-p8 y anteriores
- Adobe Commerce y Adobe Magento Open Source versión 2.4.4-p9 y anteriores

Recomendación:

Se recomienda validar si la organización cuenta con las versiones vulnerables de Adobe Commerce y Magento Open Source. De ser el caso, aplicar los parches correspondientes para solucionar estas vulnerabilidades.

URL asociado:

- https://helpx.adobe.com/security/products/magento/apsb24-61.html

ADOBE INCOPY:

CVE-2024-41858: Vulnerabilidad en Adobe InCopy permite ejecución de código arbitrario**. - (ALTA)**

Una vulnerabilidad de desbordamiento de enteros en Adobe InCopy permite que un atacante pueda ejecutar código arbitrario, luego de engañar a la víctima para que abra un archivo malicioso.

Versiones afectadas:

- Adobe InCopy versión 19.4 y anteriores
- Adobe InCopy versión 18.5.2 y anteriores

Recomendación:

Se recomienda validar si la organización cuenta con las versiones vulnerables de Adobe InCopy. De ser el caso, aplicar los parches correspondientes para solucionar esta vulnerabilidad.

URL asociado:

- https://helpx.adobe.com/security/products/incopy/apsb24-64.html

ADOBE SUBSTANCE 3D SAMPLER:

CVE-2024-41861: Vulnerabilidad en Adobe Substance 3D Sampler permite fuga de memoria**. - (MEDIA)**

Adobe Substance 3D Sampler cuenta con una vulnerabilidad de lectura fuera de límites, que puede ser aprovechada por un atacante para eludir mitigaciones como ASLR y generar una divulgación de memoria confidencial.

Versiones afectadas:

- Adobe Substance 3D Sampler versión 4.5 y anteriores

Recomendación:

Se recomienda validar si la organización cuenta con las versiones vulnerables de Adobe Substance 3D Sampler. De ser el caso, aplicar los parches correspondientes para solucionar esta vulnerabilidad.

URL asociado:

- https://helpx.adobe.com/security/products/substance3d-sampler/apsb24-65.html

ADOBE SUBSTANCE 3D DESIGNER:

CVE-2024-41864: Vulnerabilidad en Adobe Substance 3D Designer permite fuga de memoria**. - (ALTA)**

Una vulnerabilidad de escritura fuera de límites en Adobe Substance 3D Designer permite que un atacante pueda ejecutar código arbitrario, luego de que un usuario abra un archivo malicioso en un sistema vulnerable.

Versiones afectadas:

- Adobe Substance 3D Designer versión 13.1.2 y anteriores

Recomendación:

Se recomienda validar si la organización cuenta con las versiones vulnerables de Adobe Substance 3D Designer. De ser el caso, aplicar los parches correspondientes para solucionar esta vulnerabilidad.

URL asociado:

- https://helpx.adobe.com/security/products/substance3d_designer/apsb24-67.html

+51 1 225 9900
info@bafing.com
www.bafing.com
Bafing
Av. Del Parque Sur 560, San Borja, Lima,Perú