Nro. Alerta:	EC-2022-030	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	11-febrero-2022	**Vulnerabilidades en productos de Adobe**	Versión 1.0

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de incidente: Sistema y/o Software Abierto
Nivel de riesgo: Medio

II. ALERTA

Existen diferentes vulnerabilidades asociadas a los productos de ADOBE; las mismas que tienen diferentes causas raíz, relacionadas con complementos de Premier Rush, Illustrator, Photoshop, After Effects, Creative y Cloud Desktop Application.

Figura 1. Ilustración asociada a Adobe.
Fuente: Adobe

III. INTRODUCCIÓN

El 08 de febrero de 2022, la empresa de Software Adobe[1]; lanzó una serie de actualizaciones con el objetivo de mitigar diferentes vulnerabilidades existentes en sus complementos.

A continuación, se describen las versiones afectadas y los CVE asociados:

Ítem	Producto Vulnerable	Nivel de Riesgo	CVE Asociado
1	Adobe Premiere Rush 2.0 y versiones anteriores	Riesgo Medio	CVE-2022-23204
2	Illustrator 2022 26.0.2 y versiones anteriores. Illustrator 2021 25.4.3 y versiones anteriores.	Riesgo Medio	CVE-2022-23186 CVE-2022-23189 CVE-2022-23190 CVE-2022-23191 CVE-2022-23192 CVE-2022-23193 CVE-2022-23194 CVE-2022-23195 CVE-2022-23196

[1] Empresa que destaca en el mundo del software por sus programas de edición de páginas web, vídeo e imagen digital

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-030	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	11-febrero-2022	**Vulnerabilidades en productos de Adobe**	Versión 1.0

Ítem	Producto Vulnerable	Nivel de Riesgo	CVE Asociado
			CVE-2022-23197 CVE-2022-23198 CVE-2022-23199 CVE-2022-23188
3	Photoshop 2021 22.5.4 y versiones anteriores. Photoshop 2022 23.1 y versiones anteriores.	Riesgo Medio	CVE-2022-23203
4	Adobe After Effects 22.1.1 y versiones anteriores.	Riesgo Medio	CVE-2022-23200
5	Aplicación de escritorio Creative Cloud (instalador) 2.7.0.13 y versiones anteriores.	Riesgo Medio	CVE-2022-23202

Tabla 1. Vulnerabilidad asociada a Adobe

Adobe asigno a todas estas vulnerabilidades una prioridad de parcheo de 3, ya que normalmente no son productos a los que apuntan los piratas informáticos

IV. VECTOR DE ATAQUE:

En la siguiente tabla, se describen las características de estas vulnerabilidades y el vector de ataque determinado.

Ítem	CVE	Descripción	Vector de Ataque
1	CVE-2022-23204	La vulnerabilidad permite que un atacante remoto obtenga acceso a información potencialmente confidencial.	Un atacante remoto puede crear un archivo especialmente diseñado, engañar a la víctima para que lo abra, desencadenar un error de lectura fuera de los límites y leer el contenido de la memoria en el sistema.
2	CVE-2022-23186	Esta es una vulnerabilidad de ejecución de código arbitrario que existe en la decodificación de archivos de dibujo de CorelDraw (CDR) en Adobe Illustrator. Específicamente, la vulnerabilidad es causada por un archivo CDR con formato incorrecto, que provoca un acceso a la memoria de escritura fuera de los límites debido a una verificación de límites incorrecta.	Un atacante remoto puede aprovechar esta vulnerabilidad para ejecutar código arbitrario dentro del contexto de la aplicación a través de un archivo CDR manipulado.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-030	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	11-febrero-2022	**Vulnerabilidades en productos de Adobe**	Versión 1.0

Ítem	CVE	Descripción	Vector de Ataque
3	CVE-2022-23189	Esta es una vulnerabilidad de desreferencia de puntero nulo que existe en la decodificación de archivos de dibujo de AutoCAD (DWG) en Adobe Illustrator. Específicamente, la vulnerabilidad es causada por un archivo DWG con formato incorrecto, lo que provoca una desreferencia de puntero NULL.	Los atacantes pueden explotar esta vulnerabilidad con un archivo DWG manipulado, lo que podría provocar una denegación de servicio de la aplicación.
4	CVE-2022-23190	Esta es una vulnerabilidad de corrupción de memoria que existe en la decodificación de archivos de metarchivo de gráficos de computadora (CGM) en Adobe Illustrator. Específicamente, la vulnerabilidad es causada por un archivo CGM con formato incorrecto, que provoca un acceso a la memoria de lectura fuera de los límites debido a una verificación de límites incorrecta. La vulnerabilidad específica existe en el complemento 'Reader_for_CGM'.	Los atacantes pueden aprovechar esta vulnerabilidad para realizar lecturas de memoria no deseadas, lo que podría provocar una fuga de datos de memoria a través de un archivo CGM manipulado
5	CVE-2022-23191	Esta es una vulnerabilidad de corrupción de la memoria que existe en la decodificación del archivo de imagen de Macintosh (PCT) en Adobe Illustrator. Específicamente, la vulnerabilidad es causada por un archivo PCT con formato incorrecto, que provoca un acceso a la memoria de lectura fuera de los límites debido a una verificación de límites incorrecta. La vulnerabilidad específica existe en el complemento 'MPS'.	Los atacantes pueden aprovechar esta vulnerabilidad para realizar lecturas de memoria no deseadas, lo que podría provocar una fuga de datos de memoria a través de un archivo PCT manipulado.
6	CVE-2022-23192	Esta es una vulnerabilidad de corrupción de la memoria que existe en la decodificación de archivos de ilustraciones de Adobe Illustrator (AI) en Adobe Illustrator. Específicamente, la vulnerabilidad es causada por un archivo AI con formato incorrecto, que provoca un acceso a la memoria fuera de los límites debido a una verificación de límites incorrecta.	Los atacantes pueden explotar esta vulnerabilidad para lecturas de memoria no deseadas, lo que podría provocar una fuga de datos de memoria a través de un archivo de IA manipulado.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-030	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	11-febrero-2022	**Vulnerabilidades en productos de Adobe**	Versión 1.0

Ítem	CVE	Descripción	Vector de Ataque
7	CVE-2022-23193	Esta es una vulnerabilidad de corrupción de la memoria que existe en la decodificación de archivos de formato de documento portátil (PDF) en Adobe Illustrator. Específicamente, la vulnerabilidad es causada por un archivo PDF con formato incorrecto, lo que provoca un acceso a la memoria Fuera de los límites, debido a una verificación de límites incorrecta.	Los atacantes pueden explotar esta vulnerabilidad para lecturas de memoria no deseadas, lo que podría provocar una fuga de datos de memoria, a través de un archivo PDF manipulado.
8	CVE-2022-23194	Esta es una vulnerabilidad de corrupción de memoria que existe en la decodificación de archivos de metarchivo de gráficos de computadora (CGM) en Adobe Illustrator. Específicamente, la vulnerabilidad es causada por un archivo CGM con formato incorrecto, que provoca un acceso a la memoria de lectura fuera de los límites debido a una verificación de límites incorrecta. La vulnerabilidad específica existe en el complemento 'Reader_for_CGM'.	Los atacantes pueden aprovechar esta vulnerabilidad para realizar lecturas de memoria no deseadas, lo que podría provocar una fuga de datos de memoria a través de un archivo CGM manipulado.
9	CVE-2022-23195		
10	CVE-2022-23196	Esta es una vulnerabilidad de pérdida de memoria que existe en la decodificación de archivos de dibujo de CorelDraw (CDR) en Adobe Illustrator. Específicamente, la vulnerabilidad es causada por un archivo CDR con formato incorrecto, lo que provoca un acceso a la memoria fuera de los límites debido a una verificación de límites incorrecta.	Los atacantes pueden aprovechar esta vulnerabilidad para realizar lecturas de memoria no deseadas, lo que podría provocar una fuga de datos de memoria a través de un archivo CDR manipulado.
11	CVE-2022-23197		
12	CVE-2022-23198	Esta es una vulnerabilidad de desreferencia de puntero nulo que existe en la decodificación de archivos de dibujo de CorelDraw (CDR) en Adobe Illustrator. Específicamente, la vulnerabilidad es causada por un archivo CDR con formato incorrecto, lo que provoca una falta de referencia de puntero NULL.	Los atacantes pueden aprovechar esta vulnerabilidad con un archivo CDR manipulado, lo que podría provocar una denegación de servicio de la aplicación.
13	CVE-2022-23199		

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-030	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	11-febrero-2022	**Vulnerabilidades en productos de Adobe**	Versión 1.0

Ítem	CVE	Descripción	Vector de Ataque
14	CVE-2022-23188	Esta es una vulnerabilidad de desbordamiento de búfer en el complemento 'MPS' de Adobe Illustrator. Específicamente, la vulnerabilidad es causada por un archivo de imagen de imagen (PCT) de Macintosh con formato incorrecto, que provoca un acceso a la memoria de escritura fuera de los límites debido a una verificación de límites incorrecta al manipular un puntero a un búfer asignado.	Un atacante remoto puede aprovechar esta vulnerabilidad para ejecutar código arbitrario dentro del contexto de la aplicación a través de un archivo PCT manipulado.
15	CVE-2022-23203	Esta es una vulnerabilidad de desbordamiento de búfer que existe en la decodificación de archivos Universal 3D (U3D) en Adobe Photoshop. Específicamente, la vulnerabilidad es causada por un archivo U3D con formato incorrecto, que provoca un acceso a la memoria fuera de los límites debido a una verificación de límites incorrecta. La vulnerabilidad específica existe en el complemento 'U3D'.	Un atacante remoto puede aprovechar esta vulnerabilidad para ejecutar código arbitrario dentro del contexto de la aplicación a través de un archivo U3D manipulado.
16	CVE-2022-23200	Esta vulnerabilidad se debe a una falla de programación en la escritura del búfer de memoria en el aplicativo After Effects. Un atacante podría realizar ejecución remota de código (RCE) en el sistema afectado.	La explotación exitosa podría conducir a la ejecución de código arbitrario en el contexto del usuario actual.
17	CVE-2022-23202	Vulnerabilidad de elemento de ruta de búsqueda no controlada que podría conducir a la ejecución de código arbitrario en el instalador de la aplicación de escritorio Creative Cloud 2.7.0.13 y versiones anteriores en Windows.	Cualquier código se puede ejecutar a través de un elemento de ruta de búsqueda no controlado

Tabla 2. Descripción y Vector de Ataque de las vulnerabilidades.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-030	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	11-febrero-2022	**Vulnerabilidades en productos de Adobe**	Versión 1.0

V. IMPACTO:

Los impactos asociados a las vulnerabilidades se mencionan en la siguiente tabla:

Ítem	CVE	Gravedad	Solución	Impacto
1	CVE-2022-23204	Moderada	Actualizar a Adobe Premiere Rush versión 2.3	Escalada de privilegios
2	CVE-2022-23186	Crítico	Actualizar: Illustrator 2022 / 26.03 Illustrator 2021 / 25.4.4	Ejecución de código arbitrario
3	CVE-2022-23189	Importante		Aplicación de denegación de servicio
4	CVE-2022-23190	Importante		Pérdida de memoria
5	CVE-2022-23191	Importante		Pérdida de memoria
6	CVE-2022-23192	Importante		Pérdida de memoria
7	CVE-2022-23193	Importante		Pérdida de memoria
8	CVE-2022-23194	Importante		Pérdida de memoria
9	CVE-2022-23195	Importante		Pérdida de memoria
10	CVE-2022-23196	Moderada		Pérdida de memoria
11	CVE-2022-23197	Moderada		Pérdida de memoria
12	CVE-2022-23198	Moderada		Aplicación de denegación de servicio
13	CVE-2022-23199	Moderada		Aplicación de denegación de servicio
14	CVE-2022-23188	Crítico		Ejecución de código arbitrario

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-030	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	11-febrero-2022	**Vulnerabilidades en productos de Adobe**	Versión 1.0

Ítem	CVE	Gravedad	Solución	Impacto
15	CVE-2022-23203	Crítico	Photoshop 2021 / version 22.5.5 Photoshop 2022 / version 23.1.1	Ejecución de código arbitrario
16	CVE-2022-23200	Crítico	Adobe After Effects / 22.2	Ejecución de código arbitrario
17	CVE-2022-23202	Crítico	Aplicación de escritorio Creative Cloud (instalador) 2.7.0.15	Ejecución de código arbitrario

Tabla 3. Impacto de las vulnerabilidades.

VI. RECOMENDACIONES:

El EcuCert recomienda a su comunidad objetivo:

- Descargar programas y archivos de fuentes oficiales.
- Instalar las actualizaciones entregadas por el proveedor.

VII. REFERENCIAS:

Adobe. (s.f.). *Adobe*. Obtenido de Adobe: https://www.adobe.com/

Adobe, H. (10 de 02 de 2022). *Helpx Adobe*. Obtenido de Helpx Adobe: https://helpx.adobe.com/security/products/premiere_rush/apsb22-06.html

Adobe, H. (08 de 02 de 2022). *Helpx Adobe*. Obtenido de Helpx Adobe: https://helpx.adobe.com/security/products/illustrator/apsb22-07.html

AdobeHelpx. (08 de 02 de 2022). *AdobeHelpx*. Obtenido de AdobeHelpx: https://helpx.adobe.com/security/products/photoshop/apsb22-08.html

AdobeHelpx. (08 de 02 de 2022). *AdobeHelpx*. Obtenido de AdobeHelpx: https://helpx.adobe.com/security/products/after_effects/apsb22-09.html

CERT-PY. (09 de 02 de 2022). *CERT-PY*. Obtenido de CERT-PY: https://www.cert.gov.py/noticias/adobe-publica-actualizaciones-de-seguridad-para-

subsanar-multiples-vulnerabilidades

CybersecurityHelp. (08 de 02 de 2022). *CybersecurityHelp*. Obtenido de CybersecurityHelp: https://www.cybersecurity-help.cz/vdb/SB2022020843

Fortinet. (10 de 02 de 2022). *Fortinet*. Obtenido de Fortinet: https://www.fortinet.com/blog/threat-research/fortinet-security-researchers-discover-vulnerabilities-adobe-illustrator-photoshop

HKCERT. (09 de 02 de 2022). *Hong Kong Computer Emergency Response Team*. Obtenido de Hong Kong Computer Emergency Response Team: https://www.hkcert.org/security-bulletin/adobe-monthly-security-update-february-2022