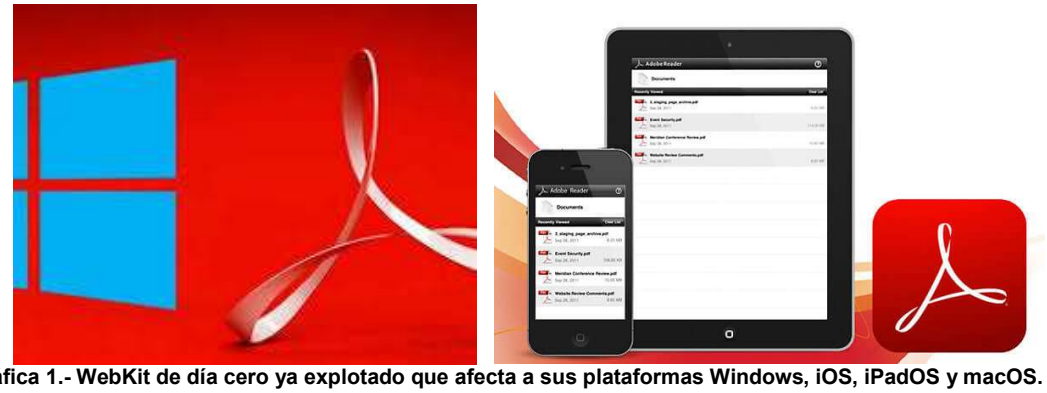
Nro. Alerta:	**AL-2023-08**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	24-febrero-2023	**Vulnerabilidad WebKit de día cero**	V 1.1

I. DATOS GENERALES.-

Clase de alerta: Vulnerabilidad
Tipo de incidente: Vulnerabilidad de día cero WebKit
Nivel de riesgo: Alta
Plataforma: Windows, MacOS, iOS, IPadOS

II. INTRODUCCIÓN.-



Gráfica 1.- WebKit de día cero ya explotado que afecta a sus plataformas Windows, iOS, iPadOS y macOS.

El fabricante de software Adobe lanzó en febrero de 2023 correcciones de seguridad para al menos media docena de vulnerabilidades que exponen a los usuarios de Windows y macOS a ataques de piratas informáticos maliciosos.

La compañía de Mountain View, California, advirtió que los problemas de seguridad existen en tres de sus productos de software más populares: Photoshop, Ilustrator y After Effects.

Según los boletines de seguridad de Adobe, los parches de Ilustrator y After Effects tienen calificaciones de gravedad crítica debido al riesgo de ataques de ejecución de código.

La compañía dijo que la vulnerabilidad de Adobe Ilustrator, rastreada como CVE-2022-23187, es un problema de desbordamiento de búfer que conduce a la ejecución de código arbitrario.

El error está presente tanto para usuarios de Windows como de macOS en Ilustrator 26.0.3 y versiones anteriores.

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:	**AL-2023-08**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	24-febrero-2023	**Vulnerabilidad WebKit de día cero**	V 1.1

Se publicó un segundo boletín crítico para cubrir al menos cuatro vulnerabilidades documentadas de Adobe After Effects que exponen a los usuarios de Windows y macOS a ataques de ejecución de código.

"Esta actualización aborda vulnerabilidades críticas de seguridad. La explotación exitosa podría llevar a la ejecución de código arbitrario en el contexto del usuario actual", dijo Adobe en un boletín que documenta desbordamientos de búfer basados en pilas con serias implicaciones.

Adobe rastrea los errores de After Effects como **CVE-2022-24094**, **CVE-2022-24095**, **CVE-2022-24096** y **CVE-2022-24097**.

La compañía también envió un tercer boletín para cubrir una falla de gravedad importante en su software insignia Adobe Photoshop.

La vulnerabilidad de Photoshop (**CVE-2022-24090**) afecta a los usuarios de Windows y macOS y Adobe advierte que la explotación exitosa podría provocar una pérdida de memoria en el contexto del usuario actual.

Adobe dijo que no estaba al tanto de ningún exploit en la naturaleza para ninguna de las fallas parcheadas este mes.

Los parches de Adobe siguen al lanzamiento de parches de Apple para cubrir un WebKit de día cero ya explotado que afecta a sus plataformas iOS, iPadOS y macOS.

La falla de WebKit, rastreada como **CVE-2023-23529**, se describe como un problema de confusión de tipos que puede explotarse para la ejecución de código arbitrario al hacer que el usuario objetivo acceda a un sitio web malicioso.

III. ALERTA.-

CVE-2023-23529

Apple ha publicado actualizaciones de seguridad que corrigen una vulnerabilidad de día cero de WebKit (CVE-2023-23529) que "puede haber sido explotada activamente".

El error se solucionó en iOS 16.3.1 y iPadOS 16.3.1, macOS Ventura 13.2.1, Safari 16.3.1 y posiblemente también en tvOS 16.3.2 y watchOS 9.3.1, aunque las notas de publicación para las actualizaciones para esos sistemas operativos de Internet de las Cosas han sido retenidos temporalmente.

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:	**AL-2023-08**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	24-febrero-2023	**Vulnerabilidad WebKit de día cero**	V 1.1

CVE-2023-23529 es un problema de confusión de tipos en WebKit, el motor del navegador que impulsa el navegador Safari y otros navegadores web que se ejecutan en iOS y iPadOS. La vulnerabilidad se desencadena al procesar contenido web creado con fines malintencionados y puede permitir que los atacantes ejecuten código arbitrario en un dispositivo vulnerable.

Se recomienda a los propietarios de iPhones, iPads y iPad minis que verifiquen las actualizaciones disponibles y actualicen sus dispositivos lo antes posible. Los usuarios de dispositivos más antiguos (p. ej., iPhone 7 y más antiguos) tendrán que esperar a que el parche se transfiera a las sucursales más antiguas de iOS y iPadOS.

Los usuarios que ejecutan macOS Ventura también obtienen un parche para CVE-2023-23529 con la actualización de seguridad del sistema operativo, mientras que aquellos que todavía usan macOS Big Sur y macOS Monterey pueden cerrar la brecha actualizando Safari a la versión 16.3.1.

La actualización de iOS y iPadOS también contiene una solución para CVE-2023-23514, un problema de uso posterior a la liberación en el kernel, que podría permitir que una aplicación maliciosa ejecute código arbitrario con privilegios del kernel.

La actualización de macOS también lo parchea, junto con un problema de privacidad en el componente Accesos directos.

IV. VECTOR DE EXPLOTACIÓN.-

- Red

V. IMPACTO.-

- CVE-2023-23529 es un problema de confusión de tipos en WebKit, el motor del navegador que impulsa el navegador Safari y otros navegadores web que se ejecutan en iOS y iPadOS. La vulnerabilidad se desencadena al procesar contenido web creado con fines malintencionados y puede permitir que los atacantes ejecuten código arbitrario en un dispositivo vulnerable.

- La vulnerabilidad se activa al procesar contenido web creado con fines malintencionados y puede permitir que los atacantes ejecuten código arbitrario en un dispositivo vulnerable.

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:	**AL-2023-08**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	24-febrero-2023	**Vulnerabilidad WebKit de día cero**	V 1.1

- Las versiones 22.2 (y anteriores) y 18.4.4 (y anteriores) de Adobe After Effects están afectadas por una vulnerabilidad de desbordamiento de búfer basado en pila que podría provocar la ejecución de código arbitrario en el contexto del usuario actual. La explotación de este problema requiere la interacción del usuario, ya que la víctima debe abrir un archivo malicioso.

- La vulnerabilidad permite que un atacante remoto ejecute código arbitrario en el sistema de destino.

- La vulnerabilidad existe debido a un error de límite al procesar archivos. Un atacante remoto puede engañar a la víctima para que abra un archivo especialmente diseñado, desencadenar un desbordamiento de búfer basado en la pila y ejecutar código arbitrario en el sistema de destino.

- La explotación exitosa de esta vulnerabilidad puede resultar en un compromiso completo del sistema vulnerable.

- La actualización de iOS y iPadOS también contiene una corrección para CVE-2023-23514, un problema de uso después de la liberación en el kernel, que podría permitir que una aplicación maliciosa ejecute código arbitrario con privilegios del kernel.

VI. INDICADORES DE COMPROMISO.-

CVE-2023-23529

Riesgo:	Alto
CVE-ID:	CVE-2023-23529
CWE-ID:	CWE-121 - Stack-based buffer overflow
Descripción:	Una condición de desbordamiento de búfer basada en pila es una condición en la que el búfer que se sobrescribe se asigna en la pila (es decir, es una variable local o, en raras ocasiones, un parámetro para una función). Los desbordamientos de búfer generalmente provocan bloqueos. Son posibles otros ataques que conducen a la falta de disponibilidad, incluido poner el programa en un bucle infinito. Los desbordamientos de búfer a menudo se pueden usar para ejecutar código arbitrario, que generalmente está fuera del alcance de la política de seguridad implícita de un programa. Cuando

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:	**AL-2023-08**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	24-febrero-2023	**Vulnerabilidad WebKit de día cero**	V 1.1

	la consecuencia es la ejecución de código arbitrario, a menudo se puede utilizar para subvertir cualquier otro servicio de seguridad. Esta debilidad se introduce durante las etapas de Arquitectura y Diseño, Implementación.
Mitigación:	El error se solucionó en iOS 16.3.1 y iPadOS 16.3.1, macOS Ventura 13.2.1, Safari 16.3.1 y posiblemente también en tvOS 16.3.2 y watchOS 9.3.1, aunque las notas de publicación para las actualizaciones para los sistemas operativos de Internet de las Cosas han sido retenidos temporalmente.
Versiones de software vulnerables	Apple ha publicado actualizaciones de seguridad que corrigen una vulnerabilidad de día cero de WebKit (CVE-2023-23529) que "puede haber sido explotada activamente".

CVE-2022-24094

Riesgo:	Alto
CVE-ID:	CVE-2022-24094
CWE-ID:	CWE-121 - Stack-based buffer overflow
Descripción:	La vulnerabilidad permite que un atacante remoto ejecute código arbitrario en el sistema de destino. La vulnerabilidad existe debido a un error de límite al procesar archivos. Un atacante remoto puede engañar a la víctima para que abra un archivo especialmente diseñado, desencadenar un desbordamiento de búfer basado en la pila y ejecutar código arbitrario en el sistema de destino. La explotación exitosa de esta vulnerabilidad puede resultar en un compromiso completo del sistema vulnerable. Las versiones 22.2 (y anteriores) y 18.4.4 (y anteriores) de Adobe After Effects están afectadas por una vulnerabilidad de desbordamiento de búfer basado en pila que podría provocar la ejecución de código arbitrario en el contexto del usuario actual. La explotación de este problema requiere la interacción del usuario, ya que la víctima debe abrir un archivo malicioso.
Mitigación:	Instalar actualizaciones desde el sitio web del proveedor.
Versiones de software vulnerables	Adobe After Effects: 22.0 - 22.2, 18.0 - 18.4.4

Nro. Alerta:	**AL-2023-08**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	24-febrero-2023	**Vulnerabilidad WebKit de día cero**	V 1.1

CVE-2022-24095

Riesgo:	Alto
CVE-ID:	CVE-2022-24095
CWE-ID:	CWE-121 - Stack-based buffer overflow
Descripción:	La vulnerabilidad permite que un atacante remoto ejecute código arbitrario en el sistema de destino. La vulnerabilidad existe debido a un error de límite al procesar archivos. Un atacante remoto puede engañar a la víctima para que abra un archivo especialmente diseñado, desencadenar un desbordamiento de búfer basado en la pila y ejecutar código arbitrario en el sistema de destino. La explotación exitosa de esta vulnerabilidad puede resultar en un compromiso completo del sistema vulnerable. Las versiones 22.2 (y anteriores) y 18.4.4 (y anteriores) de Adobe After Effects están afectadas por una vulnerabilidad de desbordamiento de búfer basado en pila que podría provocar la ejecución de código arbitrario en el contexto del usuario actual. La explotación de este problema requiere la interacción del usuario, ya que la víctima debe abrir un archivo malicioso.
Mitigación:	Instalar actualizaciones desde el sitio web del proveedor.
Versiones de software vulnerables	Adobe After Effects: 22.0 - 22.2, 18.0 - 18.4.4

CVE-2022-24096

Riesgo:	Alto
CVE-ID:	CVE-2022-24096
CWE-ID:	CWE-121 - Stack-based buffer overflow
Descripción:	La vulnerabilidad permite que un atacante remoto ejecute código arbitrario en el sistema de destino. La vulnerabilidad existe debido a un error de límite al procesar archivos. Un atacante remoto puede engañar a la víctima para que abra un archivo especialmente diseñado, desencadenar un desbordamiento de búfer basado en la pila y ejecutar código arbitrario en el sistema de destino. La explotación exitosa de esta vulnerabilidad puede resultar en un compromiso completo del sistema vulnerable. Las versiones 22.2 (y anteriores) y 18.4.4 (y anteriores) de Adobe After Effects están afectadas por una vulnerabilidad de desbordamiento de búfer basado en pila que podría provocar la

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

	ejecución de código arbitrario en el contexto del usuario actual. La explotación de este problema requiere la interacción del usuario, ya que la víctima debe abrir un archivo malicioso.
Mitigación:	Instalar actualizaciones desde el sitio web del proveedor.
Versiones de software vulnerables	Adobe After Effects: 22.0 - 22.2, 18.0 - 18.4.4

CVE-2022-24097

Riesgo:	Alto
CVE-ID:	CVE-2022-24097
CWE-ID:	CWE-121 - Stack-based buffer overflow
Descripción:	La vulnerabilidad permite que un atacante remoto ejecute código arbitrario en el sistema de destino. La vulnerabilidad existe debido a un error de límite al procesar archivos. Un atacante remoto puede engañar a la víctima para que abra un archivo especialmente diseñado, desencadenar un desbordamiento de búfer basado en la pila y ejecutar código arbitrario en el sistema de destino. La explotación exitosa de esta vulnerabilidad puede resultar en un compromiso completo del sistema vulnerable. Las versiones 22.2 (y anteriores) y 18.4.4 (y anteriores) de Adobe After Effects están afectadas por una vulnerabilidad de desbordamiento de búfer basado en pila que podría provocar la ejecución de código arbitrario en el contexto del usuario actual. La explotación de este problema requiere la interacción del usuario, ya que la víctima debe abrir un archivo malicioso.
Mitigación:	Instalar actualizaciones desde el sitio web del proveedor.
Versiones de software vulnerables	Adobe After Effects: 22.0 - 22.2, 18.0 - 18.4.4

VII. RECOMENDACIONES.-

El EcuCERT recomienda a su comunidad objetivo:

- Se recomienda a los propietarios de iPhones, iPads y iPad minis que verifiquen las actualizaciones disponibles y actualicen sus dispositivos lo antes posible. Los usuarios de dispositivos más antiguos (p. ej., iPhone 7 y más antiguos) tendrán que

esperar a que el parche se transfiera a las sucursales más antiguas de iOS y iPadOS.

- Instalar actualizaciones disponibles en medios oficiales del proveedor, previo análisis del impacto que podría provocar en los servicios críticos para el negocio de la organización.
- Realizar copias de respaldo de seguridad periódicas, de la información crítica para evitar la pérdida de la misma.
- Actualizar el sistema operativo de los equipos a las últimas versiones.
- No abrir, manipular, o interactuar, con correos electrónicos altamente sospechosos que lleguen a las bandejas de correo o mensaje en redes sociales.
- Otorgar privilegios de usuario al mínimo dependiendo del tipo de labor a realizar.
- Implementar técnicas de navegación segura en toda la Institución/Organización, como por ejemplo visita únicamente de sitios con certificados SSL, y, de origen no sospechoso.
- Bloquear el acceso de usuarios, a dispositivos de almacenamiento externo, ajenos a la Institución/Organización, a través de políticas de seguridad adecuadas.
- Implementar y monitorear, plataformas de seguridad perimetral para identificar posible tráfico malicioso tanto a nivel interno como externo a la infraestructura de red de la organización/Institución
- Descargar programas, archivos y actualizaciones, solamente desde fuentes oficiales y verificadas.
- Cerrar todo tipo de conexión/protocolo de acceso remoto a infraestructuras críticas en la Organización/Institución, en el caso de requerir su implementación, realizarlo bajo estrictas normas de seguridad apalancados en plataformas de seguridad perimetral y, uso de una VPN.
- Tener actualizado y utilizar, un software anti-virus
- Mantener actualizados, y, bajo licenciamiento, (ya sea a nivel de software libre o de paga, de ser el caso), todos y cada uno de los sistemas y subsistemas de software y hardware de toda la infraestructura de IT y OT de la Institución, esto es, incluido a nivel de Firmware de todos los componentes.
- Diseñar una política de revisión de logs, que permita detectar comportamientos fuera de lo normal en procesos legítimos del sistema.
- Mantener listas de control de acceso para las unidades mapeadas en red restringiendo los privilegios de escritura. Con esto podrá identificar el impacto generado por el cifrado de archivos, entendiendo que el secuestro de información se producirá en todas las unidades de red mapeadas en el equipo víctima.
- Capacitar a todos los usuarios, mediante la concientización y simulaciones para reconocer e informar sobre intentos de phishing e ingeniería social. Seguir las normativas internacionales tales como ISO 27001:2013 en su control A.7.2.2 “Concienciación con educación y capacitación en seguridad de la información” o NIST PR.AT-1: “Todos los usuarios se encuentran entrenados e informados”, a fin

de tener bases para divulgar campañas educativas orientadas a nivel de usuarios respecto al correcto uso de las herramientas tecnológicas
- Implementar un plan de respuesta a emergencias de la Organización/Institución.
- En el caso de sufrir un ataque de proporciones mayores, contacte a las Autoridades competentes en base a la Normativa Legal Vigente a nivel Nacional.

VIII. DESCARGO DE RESPONSABILIDAD.-

- La información en la presente alerta; se proporciona "tal cual" solo con fines informativos. EcuCERT no respalda ningún producto o servicio comercial, incluidos los sujetos de análisis.
- Cualquier referencia a productos, procesos o servicios comerciales específicos por marca de servicio, marca comercial, fabricante o de otro modo, no constituye ni implica respaldo, recomendación o favorecimiento por parte del EcuCERT.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. BIBLIOGRAFÍA.-

- **Naraine, R. (2023).** *Adobe Plugs Critical Security Holes in Illustrator, After Effects Software,* SECURITYWEEK, recuperado el 24 de febrero de 2023 de: https://www.securityweek.com/adobe-plugs-critical-security-holes-in-illustrator-after-effects-software/

- **kovacs, E. (2023).** *Apple Patches Actively Exploited WebKit Zero-Day Vulnerability ,* SECURITYWEEK, recuperado el 24 de febrero de 2023 de: https://www.securityweek.com/apple-patches-actively-exploited-webkit-zero-day-vulnerability/

- **Naraine, R. (2023).** *Microsoft Patch Tuesday: 97 Windows Vulns, 1 Exploited Zero-Day,* SECURITYWEEK, recuperado el 24 de febrero de 2023 de: https://www.securityweek.com/microsoft-patch-tuesday-97-windows-vulns-1-exploited-zero-day/

- **Naraine, R. (2023).** *Zoom Patches High Risk Flaws on Windows, MacOS Platforms,* SECURITYWEEK, recuperado el 24 de febrero de 2023 de: https://www.securityweek.com/zoom-patches-high-risk-flaws-windows-macos-platforms/

Nro. Alerta:	**AL-2023-08**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	24-febrero-2023	**Vulnerabilidad WebKit de día cero**	V 1.1

- **Naraine, R. (2023).** *Patch Tuesday: Microsoft Warns of Under-Attack Windows Kernel Flaw,* SECURITYWEEK, recuperado el 24 de febrero de 2023 de: https://www.securityweek.com/patch-tuesday-microsoft-warns-under-attack-windows-kernel-flaw/

- **Zorz, Z. (2023).** *Apple fixes actively exploited WebKit zero-day in iOS, macOS (CVE-2023-23529),* HELP NET SECURITY, recuperado el 24 de febrero de 2023 de: https://www.helpnetsecurity.com/2023/02/14/cve-2023-23529/

- **CVE MITRE. (2023).** *CVE-2022-24094,* recuperado el 24 de febrero de 2023 de: https://cve.mitre.org/cgi-bin/cvename.cgi?name=2022-24094

- **CVE MITRE. (2023).** *CVE-2022-24095,* recuperado el 24 de febrero de 2023 de: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24095

- **CVE MITRE. (2023).** *CVE-2022-24096,* recuperado el 24 de febrero de 2023 de: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24096

- **CVE MITRE. (2023).** *CVE-2022-24097,* recuperado el 24 de febrero de 2023 de: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24097

- **CVE MITRE. (2023).** *CVE-2023-23529,* recuperado el 24 de febrero de 2023 de: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23529

- **CIBERSECURITYHELP (2023).** *Multiple vulnerabilities in Adobe After Effects,* recuperado el 24 de febrero de 2023 de: https://www.cybersecurity-help.cz/vdb/SB2022030904