Alerta de Seguridad Informática

Alerta de seguridad informática	9VSA-00035-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de agosto de 2019
Última revisión	14 de agosto de 2019

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 entregada por Adobe referente vulnerabilidades detectadas en varios de sus productos y sus respectivas actualizaciones para mitigar el riesgo.

Vulnerabilidad

CVE-2019-8062 CVE-2019-8063
CVE-2019-7870 CVE-2019-7957
CVE-2019-7931 CVE-2019-7958
CVE-2019-7961 CVE-2019-7959

Impacto

Adobe After Effects versiones 16 y anteriores tienen una vulnerabilidad de carga de biblioteca insegura (secuestro de dll). La explotación exitosa podría conducir a la ejecución de código arbitrario.

Productos Afectados

Adobe After Effects CC 2019, versiones anteriores a 16.1.2 para Windows y Mac

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace

https://helpx.adobe.com/security/products/after_effects/apsb19-31.html

Vulnerabilidad

CVE-2019-7870

Impacto

Adobe Character Animator versiones 2.1 y anteriores tienen una vulnerabilidad de carga de biblioteca insegura (secuestro de dll). La explotación exitosa podría conducir a la ejecución de código arbitrario.

Productos Afectados

Adobe Character Animator CC 2019, versiones anteriores a 2.1.1 para Windows y Mac

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace

https://helpx.adobe.com/security/products/character_animator/apsb19-32.html

---

Vulnerabilidad

CVE-2019-7931

Impacto

Adobe Premiere Pro CC versiones 13.1.2 y anteriores tienen una vulnerabilidad de carga de biblioteca insegura (secuestro de dll). La explotación exitosa podría conducir a la ejecución de código arbitrario.

Productos Afectados

Adobe Premiere Pro CC 2019, versiones anteriores a 13.1.3 para Windows y Mac

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace

https://helpx.adobe.com/security/products/premiere_pro/apsb19-33.html

Vulnerabilidad

CVE-2019-7961

Impacto

Adobe Prelude CC versiones 8.1 y anteriores tienen una vulnerabilidad de carga de biblioteca insegura (secuestro de dll). La explotación exitosa podría conducir a la ejecución de código arbitrario.

Productos Afectados

Adobe Prelude CC 2019, versiones anteriores a 8.1.1 para Windows y Mac

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace

https://helpx.adobe.com/security/products/prelude/apsb19-35.html

---

Vulnerabilidad

CVE-2019-8063
CVE-2019-7957
CVE-2019-7958
CVE-2019-7959

Impacto

Creative Cloud Desktop Application versiones 4.6.1 y anteriores presenta distintas vulnerabilidades, de las cuales se señala su impacto
CVE-2019-8063 – Transmisión insegura de datos confidenciales, lo que puede provocar una fuga de información
CVE-2019-7957 – Bypass de seguridad, lo que puede provocar una denegación de servicios (DoS)
CVE-2019-7958 – Permisos heredados inseguros, lo que puede provicar una escalación de privilegios.
CVE-2019-7959 – Uso de componentes con vulnerabilidades conocidas, lo que puede provocar una ejecución de código arbitrario.

Productos Afectados

Creative Cloud Desktop Application, versiones anteriores a 4.9 para Windows y Mac

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace

https://helpx.adobe.com/security/products/creative-cloud/apsb19-39.html

---

Vulnerabilidad

Distintos vulnerabilidades que afectan a Acrobat Reader

Impacto

Out-of-Bounds Read: La vulnerabilidad permite que un atacante remoto obtenga acceso a información potencialmente confidencial. Los CVE asociados a esta vulnerabilidad son:

CVE-2019-8077	CVE-2019-8002	CVE-2019-8021
CVE-2019-8094	CVE-2019-8004	CVE-2019-8032
CVE-2019-8095	CVE-2019-8005	CVE-2019-8035
CVE-2019-8096	CVE-2019-8007	CVE-2019-8037
CVE-2019-8102	CVE-2019-8010	CVE-2019-8040
CVE-2019-8103	CVE-2019-8011	CVE-2019-8043
CVE-2019-8104	CVE-2019-8012	CVE-2019-8052
CVE-2019-8105	CVE-2019-8018	
CVE-2019-8106	CVE-2019-8020	

Out-of-Bounds Write: La vulnerabilidad permite que un atacante remoto comprometa el sistema vulnerable, por lo general, esto puede provocar la corrupción de datos, un bloqueo o la ejecución de código. Los CVE asociados a esta vulnerabilidad son:

CVE-2019-8098	CVE-2019-8016
CVE-2019-8100	CVE-2019-8022
CVE-2019-7965	CVE-2019-8023
CVE-2019-8008	CVE-2019-8027
CVE-2019-8009	

Command Injection: Una vulnerabilidad de inyección de comandos que podría permitir la ejecución de código arbitrario. El CVE asociado a esta vulnerabilidad es:
CVE-2019-8060

Use After Free: se refiere específicamente al intento de acceder a la memoria después de que se ha liberado, lo que puede hacer que un programa se bloquee o, en el caso de una falla Use-After-Free, puede resultar en la ejecución de código arbitrario o incluso habilitar capacidades completas de ejecución remota de código. Los CVE asociados a esta vulnerabilidad son:

CVE-2019-8003	CVE-2019-8031	CVE-2019-8053
CVE-2019-8013	CVE-2019-8033	CVE-2019-8054
CVE-2019-8024	CVE-2019-8034	CVE-2019-8055
CVE-2019-8025	CVE-2019-8036	CVE-2019-8056

CVE-2019-8026 CVE-2019-8038 CVE-2019-8057
CVE-2019-8028 CVE-2019-8039 CVE-2019-8058
CVE-2019-8029 CVE-2019-8047 CVE-2019-8059
CVE-2019-8030 CVE-2019-8051 CVE-2019-8061

Heap Overflow: vulnerabilidades que podrían permitir la escalada de privilegios. Los CVE asociados a esta vulnerabilidad son:
CVE-2019-7832 CVE-2019-8042
CVE-2019-8014 CVE-2019-8046
CVE-2019-8015 CVE-2019-8049
CVE-2019-8041 CVE-2019-8050

Buffer Error: Una vulnerabilidad de error de búfer que podría conducir a la ejecución de código arbitrario. El CVE asociado a esta vulnerabilidad es:
CVE-2019-8048

Double Free: Una vulnerabilidad que podría permitir la ejecución de código arbitrario. El CVE asociado a esta vulnerabilidad es:
CVE-2019-8044

Integer Overflow: La vulnerabilidad permite que un atacante remoto obtenga acceso a información confidencial. Los CVE asociados a esta vulnerabilidad son:
CVE-2019-8099 CVE-2019-8101
Internal IP Disclosure: La vulnerabilidad permite que un atacante remoto obtenga acceso a información confidencial. En este caso un atacante remoto puede obtener la dirección IP local del usuario. El CVE asociado a esta vulnerabilidad es:
CVE-2019-8097

Type Confusion: La vulnerabilidad existe debido a un error de confusión de tipos al procesar archivos PDF. Un atacante remoto puede crear un archivo PDF especialmente diseñado, engañar a la víctima para que lo abra y ejecutar código arbitrario en el sistema de destino. El CVE asociado a esta vulnerabilidad es:
CVE-2019-8019

Untrusted Pointer Dereference: la vulnerabilidad obtiene un valor de una fuente no confiable, convierte este valor en un puntero y desreferencia el puntero resultante. Los CVE asociados a esta vulnerabilidad son:
CVE-2019-8006
CVE-2019-8017
CVE-2019-8045

Productos Afectados

Acrobat DC Continuous, versiones anteriores a 2019.012.20036, para Windows y macOS
Acrobat Reader DC Continuous, versiones anteriores a 2019.012.20036, para Windows y macOS
Acrobat DC Classic 2017, versiones anteriores a 2017.011.30144, para Windows y macOS
Acrobat Reader DC Classic 2017, versiones anteriores a 2017.011.30144, para Windows y macOS
Acrobat DC Classic 2015, versiones anteriores a 2015.006.30499, para Windows y macOS

Acrobat Reader DC Classic 2015, versiones anteriores a 2015.006.30499, para Windows y macOS

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace

https://helpx.adobe.com/security/products/acrobat/apsb19-41.html

---

Vulnerabilidad

CVE-2019-7964

Impacto

Adobe ha publicado actualizaciones de seguridad para Adobe Experience Manager (AEM). Estas actualizaciones resuelven una vulnerabilidad de omisión de autenticación crítica en el controlador del Lenguaje de marcado de aserción de seguridad (SAML) en las versiones AEM 6.4 y 6.5. La explotación exitosa podría resultar en acceso no autorizado al entorno AEM.

Productos Afectados

Adobe Experience Manager, versiones 6.4 y 6.5, para todas las plataformas

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace

https://helpx.adobe.com/security/products/experience-manager/apsb19-42.html

---

Vulnerabilidad

Múltiples vulnerabilidades que afectan a Photoshop CC

Impacto

Heap Overflow: vulnerabilidades que podrían permitir la escalada de privilegios. Los CVE asociados a esta vulnerabilidad son:

CVE-2019-7978 CVE-2019-7990
CVE-2019-7980 CVE-2019-7993
CVE-2019-7985

Type Confusion: La vulnerabilidad existe debido a un error de confusión de tipos al procesar archivos PSD. Un atacante remoto puede crear un archivo PSD especialmente diseñado, engañar a la víctima para que lo abra y ejecutar código arbitrario en el sistema de destino. Los CVE asociados a esta vulnerabilidad son:

CVE-2019-7969
CVE-2019-7970
CVE-2019-7971
CVE-2019-7972
CVE-2019-7973
CVE-2019-7974
CVE-2019-7975

Out-of-Bounds Read: La vulnerabilidad permite que un atacante remoto obtenga acceso a información potencialmente confidencial. Los CVE asociados a esta vulnerabilidad son:

CVE-2019-7977
CVE-2019-7981
CVE-2019-7987
CVE-2019-7991
CVE-2019-7992
CVE-2019-7995
CVE-2019-7996
CVE-2019-7997
CVE-2019-7998
CVE-2019-7999
CVE-2019-8000
CVE-2019-8001

Command Injection: Una vulnerabilidad de inyección de comandos que podría permitir la ejecución de código arbitrario. Los CVE asociados a esta vulnerabilidad son:

CVE-2019-7968
CVE-2019-7989

Out-of-Bounds Write: La vulnerabilidad permite que un atacante remoto comprometa el sistema vulnerable, por lo general, esto puede provocar la corrupción de datos, un bloqueo o la ejecución de código. Los CVE asociados a esta vulnerabilidad son:

CVE-2019-7976
CVE-2019-7979
CVE-2019-7982
CVE-2019-7983
CVE-2019-7984
CVE-2019-7986
CVE-2019-7988
CVE-2019-7994

Productos Afectados

Photoshop CC, versiones anteriores a 19.1.9 y versiones anteriores a 20.0.6, para Windows y macOS.

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace

https://helpx.adobe.com/security/products/photoshop/apsb19-44.html