

# Alerta de Seguridad Cibernética



Alerta de seguridad informática	9VSA20-00219-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de mayo de 2020
Última revisión	20 de mayo 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 su lector PDF para Windows y MacOS. El presente informe incluye la respectiva medida de mitigación.

# Lista de CVEs













### **Vulnerabilidades**

CVE-2020-9592: Impacto crítico.

Evasión de medidas de seguridad implementadas, compromete completamente al sistema afectado.

CVE-2020-9593: Impacto importante.

Acceso de memoria inválida, permite obtención de información potencialmente sensible.

CVE-2020-9594: Impacto crítico.

Escritura fuera de los límites en memoria, permite la ejecución de código arbitrario en el sistema afectado.

CVE-2020-9595: Impacto importante.

Acceso de memoria inválida, permite obtención de información potencialmente sensible.

CVE-2020-9596: Impacto crítico.

Evasión de medidas de seguridad implementadas, compromete completamente al sistema afectado.

CVE-2020-9597: Impacto crítico.

Escritura fuera de los límites en memoria, permite la ejecución de código arbitrario en el sistema afectado.

CVE-2020-9598: Impacto importante.

Acceso de memoria inválida, permite obtención de información sensible.

CVE-2020-9599: Impacto importante.

Lectura fuera los límites de la memoria, permite la obtención de información sensible.

CVE-2020-9600: Impacto importante.

Lectura fuera los límites de la memoria, permite la obtención de información sensible.

CVE-2020-9601: Impacto importante.

Lectura fuera los límites de la memoria, permite la obtención de información sensible.

CVE-2020-9602: Impacto importante.

Lectura fuera los límites de la memoria, permite la obtención de información sensible.

CVE-2020-9603: Impacto importante.

Lectura fuera los límites de la memoria, permite la obtención de información sensible.

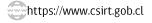
CVE-2020-9604: Impacto crítico.

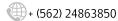
Error en el buffer. Permite a un atacante la ejecución de código arbitrario en el sistema afectado.

CVE-2020-9605: Impacto crítico.

Ministerio del Interior y Seguridad Pública

Error en el buffer. Permite a un atacante la ejecución de código arbitrario en el sistema afectado.











CVE-2020-9606: Impacto crítico.

Uso de la memoria luego de ser liberada. Permite a un atacante la ejecución de código arbitrario en el sistema afectado.

CVE-2020-9607: Impacto crítico.

Uso de la memoria luego de ser liberada. Permite a un atacante la ejecución de código arbitrario en el sistema afectado.

CVE-2020-9608: Impacto importante.

Lectura fuera los límites de la memoria, permite la obtención de información sensible.

CVE-2020-9609: Impacto importante.

Lectura fuera los límites de la memoria, permite la obtención de información sensible.

CVE-2020-9610: Impacto importante.

Puntero nulo. Permite a un atacante causar una denegación de servicios en el sistema afectado.

CVE-2020-9611: Impacto importante.

Agotamiento de la pila en memoria. Permite a un atacante causar una denegación de servicios en el sistema afectado.

CVE-2020-9612: Impacto crítico.

Desbordamiento del montículo. Permite a un atacante la ejecución de código arbitrario en el sistema afectado.

CVE-2020-9613: Impacto crítico.

Evasión de medidas de seguridad implementadas, compromete completamente al sistema afectado.

CVE-2020-9614: Impacto crítico.

Evasión de medidas de seguridad implementadas, compromete completamente al sistema afectado.

CVE-2020-9615: Impacto crítico.

Condición de carrera, permite la evasión de medidas de seguridad implementadas.

### **Productos Afectados**

Acrobat DC versión 2020.006.20042 y anteriores.

Acrobat Reader DC versión 2020.006.20042 y anteriores.

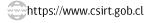
Acrobat 2017 versión 2017.011.30166 y anteriores.

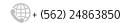
Acrobat Reader 2017 versión 2017.011.30166 y anteriores.

Acrobat 2015 2015.006.30518 y anteriores.

Ministerio del Interior y Seguridad Pública

Acrobat Reader 2015 versión 2015.006.30518 y anteriores.











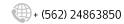
#### Mitigación

Para Acrobat DC, actualizar a la versión 2020.009.20063. Para Acrobat Reader DC, actualizar a la versión 2020.009.20063. Para Acrobat 2017, actualizar a la versión 2017.011.30171. Para Acrobat Reader 2017, actualizar a la versión 2017.011.30171. Para Acrobat 2015, actualizar a la versión 2015,006,30523. Para Acrobat Reader, actualizar a la versión 2015.006.30523.

#### **Enlaces**

https://helpx.adobe.com/security/products/acrobat/apsb20-24.html https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9592 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9593 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9594 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9595 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9596 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9597 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9598 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9599 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9600 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9601 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9602 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9603 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9604 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9605 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9606 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9607 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9608 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9609 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9610 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9611 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9612 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9613 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9614 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9615





Ministerio del Interior y Seguridad Pública



