| | |
|---|---|
| Alerta de seguridad cibernética | 9VSA20-00196-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 30 de abril de 2020 |
| Última revisión | 30 de abril 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 entregada por Adobe referente a múltiples vulnerabilidades que afectan a su producto Adobe Bridge. El presente informe incluye la respectiva medida de mitigación.

## VULNERABILIDADES

CVE-2020-9553
CVE-2020-9554
CVE-2020-9555
CVE-2020-9556
CVE-2020-9557
CVE-2020-9558
CVE-2020-9559
CVE-2020-9560
CVE-2020-9561
CVE-2020-9562
CVE-2020-9563
CVE-2020-9564
CVE-2020-9565
CVE-2020-9566
CVE-2020-9567
CVE-2020-9568
CVE-2020-9569

## CVE-2020-9553

Debido a un error en memoria, un atacante podría crear un archivo especialmente diseñado, engañar a la víctima para que lo abra y gatillar el error de lectura fuera de los límites en la memoria, permitiéndole leer contenidos del sistema que de otra forma no serían accesibles.

## CVE-2020-9554

Debido a un error en memoria al procesar datos ingresados no confiables, un atacante podría crear un archivo especialmente diseñado, engañar a la víctima para que lo abra utilizando el software afectado y gatillar el error de escritura fuera de los límites en la memoria, permitiéndole ejecutar código arbitrario en el sistema.

## CVE-2020-9555

Debido a un error en memoria, un atacante podría crear un archivo especialmente diseñado, engañar a la víctima para que lo abra y gatillar el error de desbordamiento de pila y así lograr ejecutar código arbitrario de forma remota en el sistema afectado.

## CVE-2020-9556

Debido a un error en memoria al procesar datos ingresados no confiables, un atacante podría crear un archivo especialmente diseñado, engañar a la víctima para que lo abra utilizando el software afectado y gatillar el error de escritura fuera de los límites en la memoria, permitiéndole ejecutar código arbitrario en el sistema.

## CVE-2020-9557

Debido a un error en memoria, un atacante podría crear un archivo especialmente diseñado, engañar a la víctima para que lo abra y gatillar el error de lectura fuera de los límites en la memoria, permitiéndole leer contenidos del sistema que de otra forma no serían accesibles.

## CVE-2020-9558

Debido a un error en memoria, un atacante podría crear un archivo especialmente diseñado, engañar a la víctima para que lo abra y gatillar el error de lectura fuera de los límites en la memoria, permitiéndole leer contenidos del sistema que de otra forma no serían accesibles.

## CVE-2020-9559

Debido a un error en memoria al procesar datos ingresados no confiables, un atacante podría crear un archivo especialmente diseñado, engañar a la víctima para que lo abra utilizando el software afectado y gatillar el error de escritura fuera de los límites en la memoria, permitiéndole ejecutar código arbitrario en el sistema.

## CVE-2020-9560

Debido a un error en memoria al procesar datos ingresados no confiables, un atacante podría crear un archivo especialmente diseñado, engañar a la víctima para que lo abra utilizando el software afectado y gatillar el error de escritura fuera de los límites en la memoria, permitiéndole ejecutar código arbitrario en el sistema.

## CVE-2020-9561

Debido a un error en memoria al procesar datos ingresados no confiables, un atacante podría crear un archivo especialmente diseñado, engañar a la víctima para que lo abra utilizando el software afectado y gatillar el error de escritura fuera de los límites en la memoria, permitiéndole ejecutar código arbitrario en el sistema.

## CVE-2020-9562

Debido a un error en memoria, un atacante podría crear un archivo especialmente diseñado, engañar a la víctima para que lo abra y gatillar el error de desbordamiento de pila y así lograr ejecutar código arbitrario de forma remota en el sistema afectado.

## CVE-2020-9563

Debido a un error en memoria, un atacante podría crear un archivo especialmente diseñado, engañar a la víctima para que lo abra y gatillar el error de desbordamiento de pila y así lograr ejecutar código arbitrario de forma remota en el sistema afectado.

## CVE-2020-9564

Debido a un error en memoria al procesar datos ingresados no confiables, un atacante podría crear un archivo especialmente diseñado, engañar a la víctima para que lo abra utilizando el software afectado y gatillar el error de escritura fuera de los límites en la memoria, permitiéndole ejecutar código arbitrario en el sistema.

## CVE-2020-9565

Debido a un error en memoria al procesar datos ingresados no confiables, un atacante podría crear un archivo especialmente diseñado, engañar a la víctima para que lo abra utilizando el software afectado y gatillar el error de escritura fuera de los límites en la memoria, permitiéndole ejecutar código arbitrario en el sistema.

## CVE-2020-9566

Debido a un error en memoria al procesar datos ingresados no confiables, un atacante podría crear un archivo especialmente diseñado, engañar a la víctima para que lo abra utilizando el software afectado y gatillar el error de uso de memoria luego de ser liberada, permitiéndole ejecutar código arbitrario en el sistema.

## CVE-2020-9567

Debido a un error en memoria al procesar datos ingresados no confiables, un atacante podría crear un archivo especialmente diseñado, engañar a la víctima para que lo abra utilizando el software afectado y gatillar el error de uso de memoria luego de ser liberada, permitiéndole ejecutar código arbitrario en el sistema.

## CVE-2020-9568

Debido a un error en memoria, un atacante podría crear un archivo especialmente diseñado, engañar a la víctima para que lo abra y gatillar el error en memoria y así lograr ejecutar código arbitrario de forma remota en el sistema afectado.

# CVE-2020-9569

Debido a un error en memoria al procesar datos ingresados no confiables, un atacante podría crear un archivo especialmente diseñado, engañar a la víctima para que lo abra utilizando el software afectado y gatillar el error de escritura fuera de los límites de la memoria, permitiéndole ejecutar código arbitrario en el sistema.

### Productos Afectados
Adobe Bridge versiones 10.01 y anteriores para Windows.

# MITIGACIÓN

### Mitigación
Actualizar a la versión 4.10.14, 4.11.7 ó 4.12.1.

### Enlaces
https://helpx.adobe.com/security/products/bridge/apsb20-19.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9553
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9554
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9555
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9556
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9557
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9558
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9559
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9560
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9561
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9562
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9563
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9564
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9565
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9566
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9567
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9568
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9569

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.04.30 10:49:50 -04'00'