Nro. Alerta:	EC-2022-068	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	20-may-2022	**Ejecución de código arbitrario en aplicaciones de Adobe y Word**	V 1.1

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad

Tipo de incidente: Sistemas y/o software Abierto

Nivel de riesgo: Alto

II. ALERTA

Se han detectado 134 problemas de seguridad que permiten a atacantes la ejecución de código arbitrario en dos de las aplicaciones más utilizadas en el mundo.

Figura 1.- Ilustracion de aplicaciones que presentan huecos de seguridad identificadas por Cooper
Fuente: Adslzone.net

III. INTRODUCCIÓN

Investigadores han creado una herramienta denominada “COOPER”, la que detecta fallas en la forma en que las aplicaciones Microsoft Word y Adobe Acrobat procesan JavaScript.

La herramienta COOPER, es un conjunto de secuencias de comandos (scripts), en Python, que consigue inferir en el proceso por el cual algunos scripts o aplicaciones pueden producir un comportamiento no deseado y/o peligroso. Uno de los investigadores explicó durante un evento, que tanto Word como Acrobat

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

aceptan aportes de lenguaje de scripting[1]; de hecho, Acrobat incluso permite que Javascript manipule archivos PDF; para esto, es necesario que el PDF defina objetos PDF nativos y analice el código JavaScript. Los módulos de Acrobat procesan los objetos nativos y un motor JavaScript integrado controla los scripts.

Este código según los investigadores *«es propenso a una semántica inconsistente y agujeros de seguridad, que conducen a vulnerabilidades graves»*, por lo que, dos de las vulnerabilidades encontradas en Acrobat de tipo Use After Free en la que un atacante no autenticado podría aprovechar esta vulnerabilidad para lograr la ejecución de código arbitrario en el contexto del usuario actual, ha dado una puntuación de 8.8 asociados a CVE-2021-21028 y CVE-2021-21035.

IV. VECTOR DE ATAQUE: Red

Para explotar las vulnerabilidades asociadas al CVE-2021-21028 y CVE-2021-21035, un atacante no autenticado podría lograr la ejecución de código arbitrario en el contexto del usuario actual.

La explotación de estas vulnerabilidades, requieren la interacción del usuario ya que la víctima debe abrir un archivo malicioso.

V. IMPACTO:

La ejecución de código arbitrario (ACE) es la capacidad de un atacante para ejecutar comandos o código arbitrarios en una máquina objetivo o en un proceso objetivo. Una vulnerabilidad de ejecución de código arbitrario es una falla de seguridad en el software o hardware que permite la ejecución de código

[1] Los lenguajes de secuencias de comandos (lenguajes de scripting) son de tipo específico, que se utiliza para dar instrucciones a través del código a navegadores web o aplicaciones independientes, ampliamente utilizados en desarrollo web y en los sistemas operativos para crear y au1tomatizar archivos de inicio, juegos, software de análisis estadístico, etc.

arbitrario. La capacidad de desencadenar la ejecución de código arbitrario a través de una red (especialmente a través de una red de área amplia como Internet) a menudo se denomina ejecución de código remoto (RCE).

La ejecución de código arbitrario se logra comúnmente mediante el control sobre el puntero de instrucción de un proceso en ejecución. El puntero de instrucción apunta a la siguiente instrucción del proceso que se ejecutará. Por lo tanto, el control sobre el valor del puntero de instrucción permite controlar qué instrucción se ejecuta a continuación. Para ejecutar código arbitrario, muchos exploits inyectan código en el proceso (por ejemplo, enviándole una entrada que se almacena en un búfer de entrada en la RAM) y usan una vulnerabilidad para cambiar el puntero de la instrucción para que apunte al código inyectado. El código inyectado se ejecutará automáticamente. Este tipo de ataque aprovecha que la mayoría de las computadoras no hacen una distinción general entre código y datos, el modo que el código malicioso puede camuflarse como datos de entrada inofensivos.

Por sí solo, un exploit de ejecución de código arbitrario le dará al atacante los mismos privilegios que tiene el usuario; por esta razón, una vez que un atacante puede ejecutar código arbitrario en un objetivo, a menudo intenta una explotación de escalada de privilegios para obtener un control adicional.

Para la detección de vulnerabilidades, la herramienta Cooper realiza pruebas de mutación[2] cooperativa para examinar el código vinculante de los lenguajes de secuencias de comandos para encontrar problemas de memoria segura. La mutación cooperativa modifica simultáneamente el código del script y los objetos del documento relacionado para explorar varias rutas del código vinculante. Para respaldar la mutación cooperativa, se infiere la relación entre el código y los objetos del documento.

La descripción general de Cooper se ilustra en la figura 2:

[2] La prueba de mutaciones es una técnica que trata de evaluar la efectividad de los conjuntos de casos de prueba detectando fallos insertados intencionadamente; consiste en introducir simples cambios sintácticos en el programa original mediante los operadores de mutación. Cada uno de estos cambios genera un nuevo programa al que se le conoce como mutante. Un buen conjunto de casos de prueba para un programa debe poder detectar todos los cambios que afecten a su funcionamiento.

Nro. Alerta:	EC-2022-068	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	20-may-2022	**Ejecución de código arbitrario en aplicaciones de Adobe y Word**	V 1.1

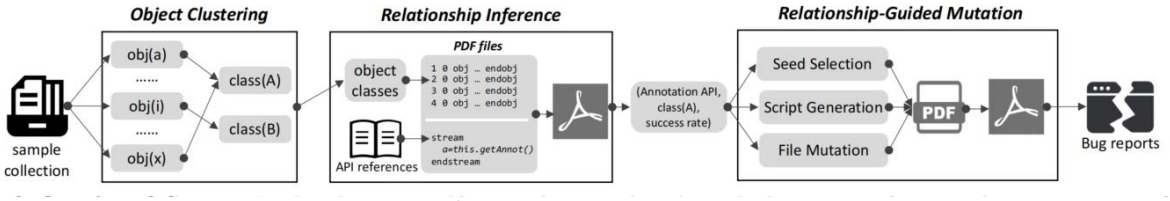

Figura 2.- *Descripción general de Cooper* **Fuente:** GitHub, Inc

COOPER agrupa los objetos en función de su semántica de alto nivel; luego infiere la relación entre los objetos y las API de secuencias de comandos. Tales relaciones ayudan a COOPER a mutar cooperativamente objetos y código de script. El documento generado se envía al programa de destino para desencadenar errores.

Las vulnerabilidades asociadas a los CVEs: CVE-2021-21028 y CVE-2021-21035 afectan a las siguientes versiones de Acrobat Reader DC:

CVEs asociados	Veresiones afectadas	Confidencialidad	Integridad	Disponibilidad	Score
CVE-2021-21028 y CVE-2021-21035	2020.013.20074 y versiones anteriores 2020.001.30018 y versiones anteriores 2017.011.30188 y versiones anteriores	Alto	Alto	Alto	8.8

COOPER ha encontrado 134 errores, 59 de ellos considerados por parte de los proveedores para dar una solución, 33 asignados un número de CVE, y 17 a los que se ha ofrecido recompensa para su solución. A continuación, se enlista los 33 CVEs asociados:

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-2022-068	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	20-may-2022	**Ejecución de código arbitrario en aplicaciones de Adobe y Word**	V 1.1

Adobe Acrobat

ID	Bug Type	Impact	Severity	CVE #	Related APIs
1	use-after-free	arbitrary code execution	High	CVE-2020-3748	Annot.page
2	use-after-free	arbitrary code execution	High	CVE-2021-21035	Annot.popupOpen ...
3	use-after-free	arbitrary code execution	High	CVE-2021-21033	Annot.setProps
4	use-after-free	arbitrary code execution	High	CVE-2021-21028	Annot.getProps ...
5	use-after-free	arbitrary code execution	High	CVE-2021-21021	Doc.getAnnots
6	use-after-free	arbitrary code execution	High	CVE-2021-35981	App.LanchURL
7	use-after-free	arbitrary code execution	High	CVE-2021-28635	Doc.addField
8	heap buffer overflow	arbitrary code execution	High	CVE-2021-28638	Doc.zoomType
9	stack buffer overflow	arbitrary code execution	High	CVE-2020-3799	Doc.getNthFieldName ...
10	buffer error	arbitrary code execution	High	CVE-2020-9698	-
11	buffer error	arbitrary code execution	High	CVE-2020-9699	-
12	buffer error	arbitrary code execution	High	CVE-2020-9700	-
13	buffer error	arbitrary code execution	High	CVE-2020-9701	Doc.getLegalWarnings
14	buffer error	arbitrary code execution	High	CVE-2020-9704	Doc.exportAsFDFStr
15	heap buffer overflow	arbitrary code execution	High	CVE-2021-28561	Doc.zoomType
16	null pointer deference	denial-of-service	Moderate	CVE-2021-39849	Annot.stateModel
17	null pointer deference	denial-of-service	Moderate	CVE-2021-39850	Annot.setProps ...
18	null pointer deference	denial-of-service	Moderate	CVE-2021-39851	Annot.popupOpen
19	null pointer deference	denial-of-service	Moderate	CVE-2021-39852	Field.getItemAt ...
20	null pointer deference	denial-of-service	Moderate	CVE-2021-39853	-
21	null pointer deference	denial-of-service	Moderate	CVE-2021-39854	Doc.zoomType
22	stack exhaustion	denial-of-service	Moderate	CVE-2020-9702	Doc.getLegalWarnings
23	stack exhaustion	denial-of-service	Moderate	CVE-2020-9703	Doc.layout ...

Figura 3.- *CVEs asociados a vulnerabilidades en Acrobat* **Fuente:** *GitHub, Inc.*

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-2022-068	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	20-may-2022	**Ejecución de código arbitrario en aplicaciones de Adobe y Word**	V 1.1

Foxit Reader

ID	Bug Type	Impact	Severity	CVE #	Related APIs
1	use-after-free	arbitrary code execution	High	CVE-2021-31441	Annot.destroy
2	use-after-free	arbitrary code execution	High	CVE-2021-31451	Annot.destroy
3	use-after-free	arbitrary code execution	High	CVE-2021-31456	Annot.popupOpen ...
4	use-after-free	arbitrary code execution	High	CVE-2021-31457	Annot.destroy
5	use-after-free	arbitrary code execution	High	CVE-2021-31458	Annot.destroy
6	use-after-free	arbitrary code execution	High	CVE-2021-34831	Field.richText ...
7	use-after-free	arbitrary code execution	High	CVE-2021-34832	Annot.readonly ...
8	use-after-free	arbitrary code execution	High	CVE-2021-34852	Field.delay ...
9	use-after-free	arbitrary code execution	High	CVE-2021-34974	Annot.delay ...
10	use-after-free	arbitrary code execution	High	CVE-2021-34975	Annot.trasitionToStat ...

Figura 4.- *CVEs asociados a vulnerabilidades en Foxit Reader* **Fuente:** *GitHub, Inc*

VI. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo tomar en consideración lo siguiente:

- Actualizar los aplicativos a las últimas versiones proporcionada por los fabricantes.
  En el caso de Acrobat los usuarios pueden actualizar en la opción Ayuda > Buscar actualizaciones; los productos se actualizarán automáticamente sin necesidad de intervención del usuario.

- Revisar contantemente el catálogo de actualizaciones y avisos de seguridad emitidos pos los fabricantes.

VII. 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.

Nro. Alerta:	EC-2022-068	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	20-may-2022	**Ejecución de código arbitrario en aplicaciones de Adobe y Word**	V 1.1

- 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.

VIII. REFERENCIAS:

- Adobe. (s.f.). *Adobe*. Obtenido de https://helpx.adobe.com/security/products/acrobat/apsb21-09.html
- Corporation., T. M. (s.f.). *The MITRE Corporation.* Obtenido de https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21035
- Corporation., T. M. (s.f.). *The MITRE Corporation.* Obtenido de https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21028
- GitHub, I. (s.f.). *GitHub, Inc.* . Obtenido de https://github.com/TCA-ISCAS/Cooper/blob/master/cve-list.md
- hmong.es. (s.f.). *hmong.es*. Obtenido de https://hmong.es/wiki/Arbitrary_code
- Incibe. (s.f.). *Incibe*. Obtenido de https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2021-21028
- Lorente, J. (22 de mayo de 2022). *adslzone.net*. Obtenido de https://www.adslzone.net/noticias/seguridad/134-agujeros-seguridad-word-adobe-acrobat/
- Nist. (s.f.). *Nist*. Obtenido de https://nvd.nist.gov/vuln/detail/CVE-2021-21028
- Peng Xu, Y. W. (s.f.). *COOPER: Testing the Binding Code of Scripting Languages with Cooperative Mutation*. Obtenido de https://huhong789.github.io/papers/xu:cooper.pdf
- Sharwood, S. (13 de mayo de 2022). *The Register*. Obtenido de https://www.theregister.com/2022/05/13/cooperative_mutation_flaw_finder/

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