Nro. Alerta:	EC-2021-035	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	22-dic-2021	**Exploit elude parche de seguridad de CVE-2021-40444**	V 1.0

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad

Tipo de incidente: Sistemas vulnerables

Nivel de riesgo: Alto

II. ALERTA

Sophos Labs; a través de su grupo de investigación ha detectado un Exploit, que elude el parche de seguridad de una vulnerabilidad asociada a CVE-2021-40444.

Figura 1.- lustración relacionada al exploit elude parche de seguridad de CVE-2021-40444
Fuente: Sophos Labs

III. INTRODUCCIÓN

El pasado 07 de septiembre de 2021, se publicó la vulnerabilidad de ejecución remota de código MSHTML de Microsoft cuya asignación de CNA es CVE-2021-40444; la misma que presenta las siguientes características:

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-2021-035	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	22-dic-2021	**Exploit elude parche de seguridad de CVE-2021-40444**	V 1.0

Tabla 1. Características CVE-2021-40444

Métrica	Valor / Descripción
Métrica de puntuación base	8
Vector de Ataque	Red
Productos Afectados	Sistemas operativos Windows 7 a 10. Windows Server 2008 a 2019.
Impacto	Permite la ejecución remota de código que afecta a MSHTML motor del navegador Internet Explorer pero que también es usado por los programas de Office. La vulnerabilidad puede ser explotada a través de documentos de Office especialmente diseñados para tal efecto.
Confidencialidad	Bajo, hay cierta pérdida de confidencialidad.
Integridad	Alta, hay una pérdida total de integridad o una pérdida total de protección.
Disponibilidad	Bajo, el rendimiento se reduce o hay interrupciones en la disponibilidad de recursos.
Mitigación	El 15 de septiembre de 2021, Microsoft publicó un parche para esta vulnerabilidad.

Fuente: Microsoft Security Response Center

El parche de seguridad publicado en septiembre de 2021 corrigió:

- Sesenta y seis (66) vulnerabilidades de distintos productos de Microsoft.
- "Cerrar" la brecha de la vulnerabilidad CVE-2021-40444; recordemos que en las versiones iniciales de los exploits, un documento malicioso de Office recuperaba una carga útil de malware empaquetada en un archivo Microsoft Cabinet (o .CAB).

Sin embargo, a pesar de existir un parche oficial la vulnerabilidad persiste; los investigadores de Sophos Labs a partir de una recolección de correos electrónicos del mes de octubre de 2021, determinaron una escalada del abuso del atacante.

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-2021-035	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	22-dic-2021	**Exploit elude parche de seguridad de CVE-2021-40444**	V 1.0

IV. VECTOR DE ATAQUE: Red

Para aprovechar la vulnerabilidad, los atacantes:

- Envían un correo electrónico a la víctima incluyendo un archivo RAR.
- El archivo RAR incluye un script escrito en notación Windows Scripting Host, con el documento malicioso de Word.
- A continuación, se solicita que se descomprima el documento de Word en la misma carpeta donde está almacenado el archivo RAR.
- La apertura del documento de Word desencadenará una secuencia de comandos de front-end, lo que finalmente provocará una infección con el malware Formbook.

En la siguiente figura se indica la manera de trabajo del exploit que evade con éxito el parche oficial de la vulnerabilidad CVE-2021-40444.

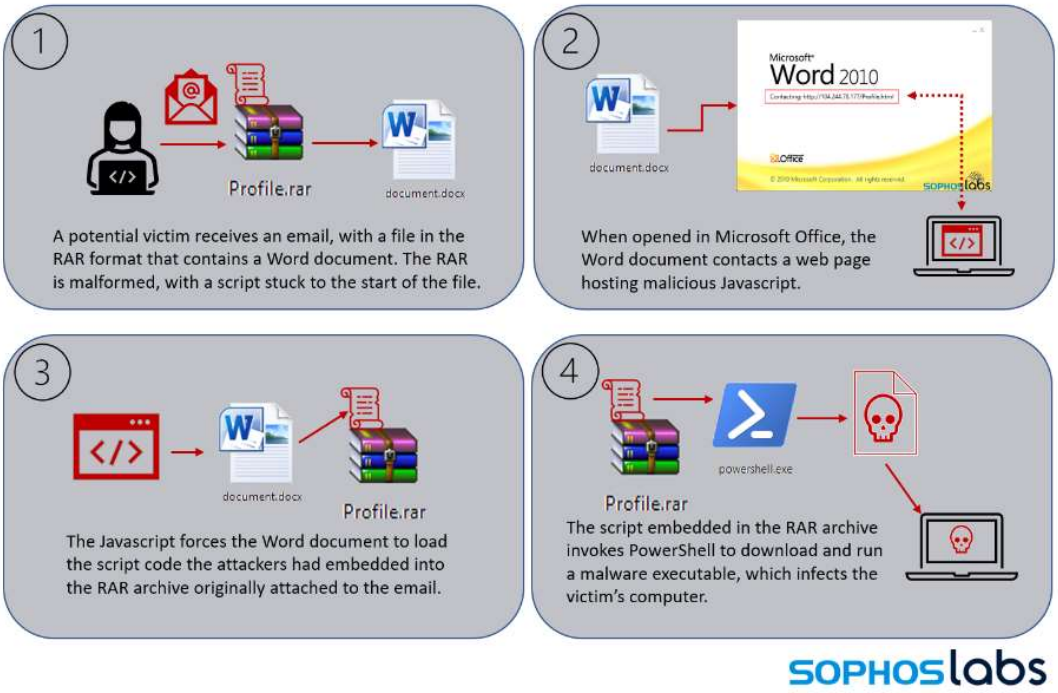

Figura 2- Vulneración del parche de seguridad CVE-2021-40444.
Fuente: Sophos Labs

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-2021-035	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	22-dic-2021	**Exploit elude parche de seguridad de CVE-2021-40444**	V 1.0

V. IMPACTO:

• A pesar de que este exploit desapareció después de solo un día de uso, se prevé que esta ejecución en seco podría volver en incidentes futuros y las alertas se activan ya que una vulnerabilidad elude un parche oficial; razón por la cual se consideran los siguientes impactos:

- Confidencialidad: Bajo, hay cierta pérdida de confidencialidad.
- Integridad: Alta, hay una pérdida total de integridad o una pérdida total de protección.
- Disponibilidad: Bajo, el rendimiento se reduce o hay interrupciones en la disponibilidad de recursos.

VI. RECOMENDACIONES:

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

- No abrir, manipular, o interactuar con correos electrónicos sospechosos recibidos en las respectivas bandejas de correo ya sea personales o Institucionales.

- Capacitar a todos los usuarios, mediante la concientización y simulaciones para reconocer e informar sobre intentos de phishing e ingeniería social.

VII. REFERENCIAS:

Brandt, A., & Holloway, R. (21 de 12 de 2012). SOPHOS NEWS. Obtenido de SOPHOS NEWS: https://news.sophos.com/en-us/2021/12/21/attackers-test-cab-less-40444-exploit-in-a-dry-run/

Center, M. S. (15 de 09 de 2021). Microsoft Security Response Center. Obtenido de Microsoft Security Response Center: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40444

ESET. (15 de 09 de 2021). Welivesecurity. Obtenido de Welivesecurity: https://www.welivesecurity.com/la-es/2021/09/15/microsoft-lanza-parche-repara-zero-day-mshtml-windows/

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