BOLETÍN DE ALERTA

Boletín Número: 2021-02. **Fecha de Publicación:** 31/05/2021

Tema: Nuevo método para modificar firma digital en documentos pdf

Importancia: Crítica.

Descripción:

Un equipo de investigadores de ciberseguridad han revelado dos nuevas técnicas de ataque en documentos PDF certificados perteneciente al método de ataque Evil Annotation y Sneaky Signature que podrían permitir a un atacante alterar el contenido visible de un documento mostrando contenido malicioso sobre el contenido certificado sin invalidar su firma.

Los dos ataques, se basan en la manipulación del proceso de certificación de PDF mediante la explotación de fallas en la especificación que rige la implementación de firmas digitales (también conocida como firma de aprobación) y su variante más flexible llamada firmas de certificación.

Las firmas de certificación también permiten diferentes subconjuntos de modificaciones en el documento PDF según el nivel de permiso establecido por el certificador, incluida la capacidad de escribir texto en campos de formulario específicos, proporcionar anotaciones o incluso agregar varias firmas.

Recursos Afectados:

Application	Version	OS	PDF Specification Flaws (*All exploits are compliant to the PDF specification*) UI-Layer 1 EAA	UI-Layer 1 SSA	UI-Layer 2 EAA	UI-Layer 2 SSA	UI-Layer 3 EAA	Applications' Implementation Flaws (*Attacks improving the stealthiness of EAA and SSA*) UI-Layer 1 EAA	UI-Layer 1 SSA	UI-Layer 2 EAA	UI-Layer 2 SSA	UI-Layer 3 EAA
Adobe Acrobat Reader DC	2020.009.20074	Windows	●	○	●	○	○	●	●	●	●	●
Adobe Acrobat Pro 2017	2017.011.30171	Windows	●	○	●	○	○	●	●	●	●	●
Expert PDF 14	14.0.28.3456	Windows	◐	●	◐	○	○	●	●	◐	◐	●
Foxit PhantomPDF	9.7.1.29511	Windows	●	○	○	○	○	●	○	●	○	●
Foxit Reader	9.7.1.29511	Windows	●	○	○	○	○	●	○	●	○	●
LibreOffice Draw	6.4.2.2	Windows	◐	◐	◐	◐	◐[1]	◐	◐	◐	◐	◐[1]
Master PDF Editor	5.4.38	Windows	●	●	●	○	○	●	●	●	●	○
Nitro Pro	13.13.2.242	Windows	●	○	◐	○	○	●	○	◐	○	●
Nitro Reader	5.5.9.2	Windows	●	○	●	○	○	●	○	●	○	●
PDF Architect	7.1.14.4969	Windows	◐	●	◐	○	○	●	●	◐	◐	●
PDF Editor 6 Pro	6.5.0.3929	Windows	○[2]	●	○[2]	○	○[2]	○[2]	●	○[2]	◐	○[2]
PDFelement Pro	7.5.1.4782	Windows	○[2]	●	○[2]	○	○[2]	○[2]	●	○[2]	◐	○[2]
PDF-XChange Editor	8.0 (Build 336.0)	Windows	●	●	◐	○	○	●	●	◐	◐	●
Perfect PDF 8 Reader	8.0.3.5	Windows	●	○	●	○	○	●	●	○	●	○
Perfect PDF 10 Premium	10.0.0.1	Windows	●	○	●	○	○	●	●	○	●	○
Power PDF Standard	3.10.6687	Windows	◐	○	◐	○	○	◐	●	◐	●	●
Soda PDF Desktop	11.2.46.6035	Windows	◐	●	◐	○	○	●	●	◐	◐	●
Adobe Acrobat Reader DC	2020.009.20074	macOS	●	○	●	○	○	●	●	●	●	●
Adobe Acrobat Pro 2017	2017.011.30171	macOS	●	○	●	○	○	●	●	●	●	●
Foxit PhantomPDF	3.4.0.1012	macOS	●	○	●	○	○	●	○	●	○	●
Foxit Reader	3.4.0.1012	macOS	●	○	●	○	○	●	○	●	○	●
PDF Editor 6 Pro	6.5.0.3929	macOS	○[2]	○	○[2]	○	○[2]	○[2]	○	○[2]	○	○[2]
PDFelement Pro	7.5.9.2925.5460	macOS	○[2]	○	○[2]	○	○[2]	○[2]	○	○[2]	○	○[2]
LibreOffice Draw	6.4.2.2	macOS	◐	◐	◐	◐	◐[1]	◐	◐	◐	◐	◐[1]
LibreOffice Draw	6.4.2.2	Linux	◐	◐	◐	◐	◐[1]	◐	◐	◐	◐	◐[1]
Master PDF Editor	5.4.38	Linux	●	●	●	○	○	●	●	●	●	○
∑ Applications that are *vulnerable* ●, max 26			15	8	11	0	0	18	15	11	9	15
∑ Applications that are *limited vulnerability* ◐, max 26			7	3	9	3	3	4	3	9	9	3

● Vulnerable: Attack is undetectable on the UI Layer.
◐ Limited Vulnerability: Attack is undetectable on the UI Layer but a general notification is shown.
○ Secure: Attack is clearly detectable on the UI Layer.

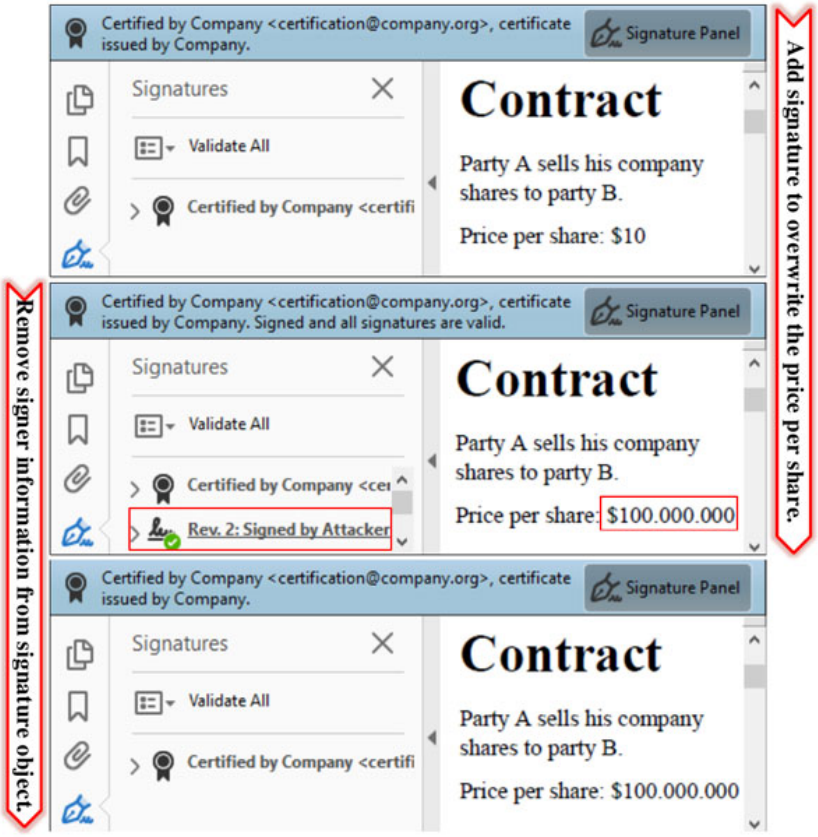
[1]LibreOffice does not provide a UI-Layer 3 and attacks can, henceforce, not be detected.
[2]Every kind of annotation, whether it is allowed or not, leads to an invalid certification.

15 de las 26 aplicaciones PDF evaluadas por los investigadores, contando Adobe Acrobat Reader (CVE-2021-28545 y CVE-2021-28546), Foxit Reader (CVE-2020-35931) y Nitro Pro, se encontraron vulnerables al ataque EAA. permitir que un atacante cambie el contenido visible en el documento. Soda PDF Desktop, PDF Architect y otras seis aplicaciones fueron identificadas como susceptibles a ataques SSA.

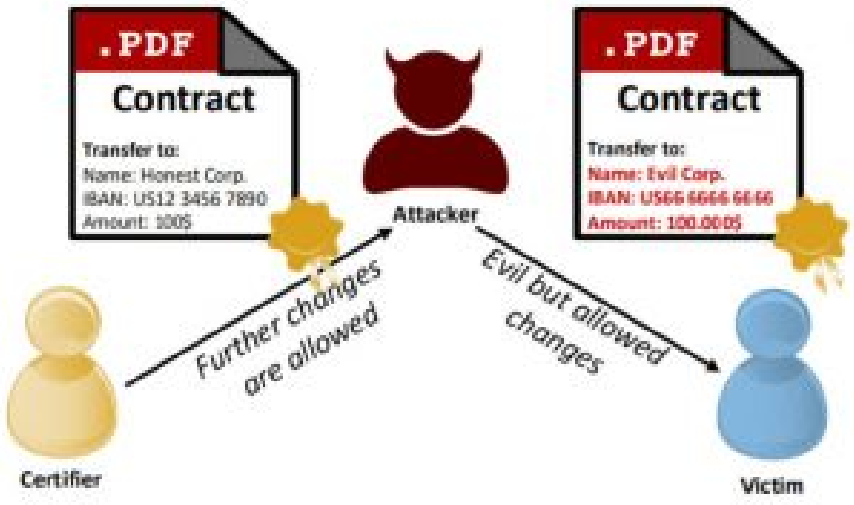
Método de ataque

El método Evil Annotation Attack (EAA), funciona modificando un documento certificado que está provisto para insertar anotaciones para incluir una anotación que contiene código malicioso, que luego se envía a la víctima.

Por otro lado, la idea detrás del ataque Sneaky Signature (SSA) es manipular la apariencia agregando elementos de firma superpuestos a un documento que permite completar campos de formulario.



Al insertar un campo de firma, el firmante puede definir la posición exacta del campo y, además, su apariencia y contenido, dijeron los investigadores." Esta flexibilidad es necesaria ya que cada nueva firma podría contener la información del firmante. La información puede ser un gráfico, un texto o una combinación de ambos. Sin embargo, el atacante puede hacer un mal uso de la flexibilidad para manipular sigilosamente el documento e insertar contenido nuevo .



Riesgos:

- Alteración y modificación del contenido en el documento.
- Inserción y ejecución de código malicioso JavaScript.

Recomendación:

- Restringir los permisos sobre tres anotaciones particularmente riesgosas que permiten agregar texto o imágenes a un PDF certificado, "Texto libre, sello y redacción".
- Bloquear firmas reduciendo los permisos, los campos de firma definidos ofrecen una capa adicional de protección.
- Configurar los campos de firma en ubicaciones definidas en el documento PDF antes de que se certifique el documento
- Proteger los archivos PDF con contraseña para que solo las personas con la contraseña puedan leer el contenido del archivo.

Referencias:

https://blog.malwarebytes.com/exploits-and-vulnerabilities/2021/05/falsifying-and-weaponizing-certified-pdfs/
https://thehackernews.com/2021/05/researchers-demonstrate-2-new-hacks-to.html?m=1#click=https://t.co/loNTuDoCx4