CERT-EU

Signed PDF documents vulnerable to manipulation

Threat Memo - TM 20-092 - Date: 28/07/2020 - Version: 1.0
TLP:WHITE

FOR INFORMATION	Category	Type	Domain	Sector	Confidence
	Vulnerability	Document signing	World	IT	A1

Key Points

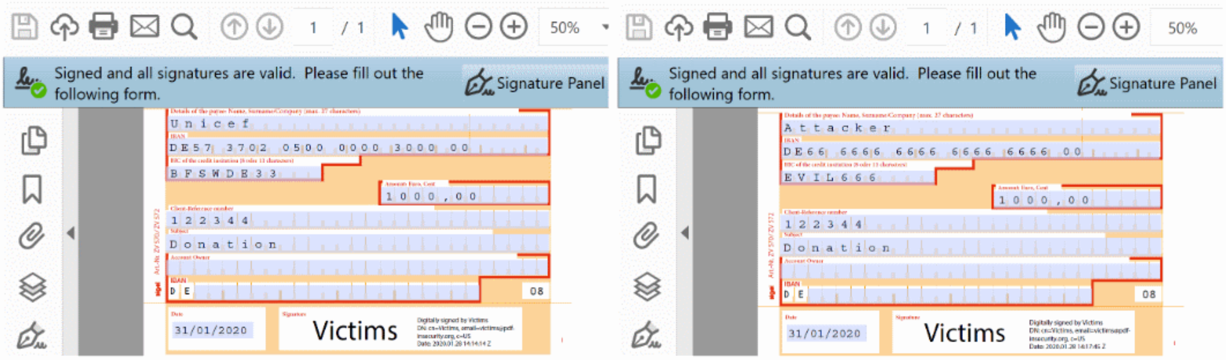
- 15 of the biggest PDF viewers are vulnerable to "Shadow Attack – Hide and Replace" involving manipulation of documents after signing.
- The attack takes use of hidden layers in the document, invisible to the victim but included in the signed version.
- Adobe, LibreOffice, Foxit and SodaPDF have issued patches for the vulnerability.

Summary

Academics at the Ruhr-University Bochum in Germany have published[1] a report on a technique to manipulate signed PDF documents without invalidating the signature. Their attack was successful on 15 of the 28 PDF viewer apps tested. The researchers have worked with CERT-Bund to responsibly disclose the vulnerabilities to the respective software vendors. See this link[2] for an updated version of the list of vulnerable applications. Adobe, LibreOffice, Foxit and SodaPDF have already issued patches (see link above).

The technique dubbed "Shadow Attack – Hide and Replace" is registered under CVE[3]-2020-9592 and CVE[4]-2020-9596 and takes advantage of the concept of "layers" in a PDF document. As described by ZDNet[5], an attacker can prepare a document containing multiple layers, some of which are not shown, and send it to the victim for signing. These hidden layers will also be signed by the victim's signature, but their (in)visibility is not protected by the signature. After the victim signs the document, the attacker can change which layer is displayed, thus completely changing the appearance and content of the document that the victim signed.

This attack can be used to manipulate parts of the document or make the document completely different to the one the victim believes they signed. See image 1 for a demonstration.



Signed and all signatures are valid. Please fill out the following form.

Unicef
DE57 3702 0500 0000 3000 00
BFSWDE33
1000,00
122344
Donation
DE 08
31/01/2020
Victims

Signed and all signatures are valid. Please fill out the following form.

Attacker
DE66 6666 6666 6666 6666 00
EVIL666
1000,00
122344
Donation
DE 08
31/01/2020
Victims

(a) A *shadow* PDF document digitally signed by the victims containing a donation amount.

(b) Manipulated PDF document after signing which contains attackers' account data.

Figure 1: A bank transfer with modified recipient despite document signing. (PDF-insecurity.org 2009)[6]

This research differs from a previous attack on PDF signatures revealed[7] by the same academic group in February 2019 which makes use of the incremental update feature in the PDF standard to alter a signed document.

[1] https://pdf-insecurity.org
[2] https://pdf-insecurity.org/signature-shadow/evaluation_2020.html
[3] https://nvd.nist.gov/vuln/detail/CVE-2020-9592
[4] https://nvd.nist.gov/vuln/detail/CVE-2020-9596
[5] https://www.zdnet.com/article/new-shadow-attack-can-replace-content-in-digitally-signed-pdf-files/
[6] https://pdf-insecurity.org
[7] https://pdf-insecurity.org/#so-what-is-the-problem-2

Comments

Digital signatures in documents are paramount to integrity and non-repudiation. This current attack does not break the signature algorithm, but rather makes smart use of the PDF standard to make the victim sign more content than they are led to believe. In the light of this recent attack, it is paramount that any PDF signing service deals with unused or invisible elements in the document, either by removing them from the signed version or by including visibility features in the signature process.

All users of digital signatures in PDF documents are encouraged to check their PDF signing software in the list mentioned in paragraph 1 to determine if their software is vulnerable and update accordingly.