Vulnerabilidades de suplantación de firmas digitales descubiertas en OpenOffice y LibreOffice

Autor: I. Stepanenko

Fecha: Sunday 24th of October 2021 06:39:01 AM

Los mantenedores de LibreOffice y OpenOffice enviaron actualizaciones de seguridad a su software de productividad para corregir múltiples vulnerabilidades que podrían ser armadas por actores malintencionados para alterar documentos y hacerlos parecer como si estuvieran firmados digitalmente por una fuente confiable.

La lista de las tres vulnerabilidades es la siguiente:

CVE-2021-41830 / CVE-2021-25633 – Manipulación de contenido y macros con ataque de certificado doble
CVE-2021-41831 / CVE-2021-25634 – Manipulación de marca de tiempo con envoltura de firma
CVE-2021-41832 / CVE-2021-25635 – Manipulación de contenido con ataque de validación de certificados
La explotación exitosa de las vulnerabilidades podría permitir a un atacante manipular la marca de tiempo de los documentos ODF firmados y, lo que es peor, alterar el contenido de un documento o autofirmar un documento con una firma que no es de confianza, que luego se modifica para cambiar el algoritmo de firma a uno no válido o algoritmo desconocido.

En los dos últimos escenarios de ataque, derivados de una validación incorrecta del certificado, LibreOffice muestra de forma incorrecta un indicador firmado válido que sugiere que el documento no ha sido manipulado desde que se firmó y presenta una firma con un algoritmo desconocido como una firma legítima emitida por una emisora de confianza.

Las vulnerabilidades se han corregido en OpenOffice versión 4.1.11 y LibreOffice versiones 7.0.5, 7.0.6, 7.1.1 y 7.1.2. A la Cátedra de Seguridad de Redes y Datos (NDS) de la Universidad de Ruhr en Bochum, se le atribuye el mérito de haber descubierto e informado sobre las tres vulnerabilidades.

Los hallazgos son los últimos de una serie de vulnerabilidades descubiertas por los investigadores de Ruht-University Bochum y siguen técnicas de ataque similares reveladas a inicios del año, que podrían permitir a un atacante modificar el contenido visible de un documento PDF certificado mostrando contenido malicioso sobre el contenido certificado sin invalidar su firma.

Se recomienda a los usuarios de LibreOffice y OpenOffice que actualicen a la última versión para mitigar el riesgo asociado con las vulnerabilidades.