Alerta de seguridad cibernética	9VSA20-00240-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de junio de 2020
Última revisión	09 de junio de 2020

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información obtenida de The Document Foundation referente a dos vulnerabilidades que afectan a su paquete de oficina libre, LibreOffice. El presente informe incluye las respectivas medidas de mitigación.

Vulnerabilidades

CVE-2020-12802
CVE-2020-12803

CVE-2020-12802

El modo sigiloso en LibreOffice hace que solo los documentos provenientes de localidades consideradas "confiables" puedan obtener recursos remotos. Esta opción no viene por defecto, pero se puede activar para no incluir los recursos de lugares no confiables. Debido a un error, los enlaces remotos gráficos cargados de archivos "docx" son omitidos de esta protección.

Productos Afectados
LibreOffice versión 6.4.3 y anteriores.

Mitigación
Actualizar a la versión 6.4.4 de LibreOffice.

Enlaces
https://www.libreoffice.org/about-us/security/advisories/cve-2020-12802/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12802

CVE-2020-12803

Los archivos ODF cuentan con formularios que pueden ser llenados por usuarios, y al igual que los formularios HTML, se pueden enviar los datos obtenidos a través de una URI, por ejemplo a un sitio web. Para realizar esto, se utiliza “Xforms W3C standard”, lo cual permite realizar el envío de datos sin el uso de macros ni programación. El problema es que esto también permitía utilizar rutas de directorios, como por ejemplo, para sobrescribir archivos locales del sistema.
A pesar de que esto solo es explotable con interacción humana (osea, no con scripts automáticos, por el momento), se subsanó la vulnerabilidad forzando a las URIs a utilizar “http”, eliminando la posibilidad de interactuar con archivos del sistema.

Productos Afectados
LibreOffice versión 6.4.3 y anteriores.

Mitigación
Actualizar a la versión 6.4.4 de LibreOffice.

Enlaces
https://www.libreoffice.org/about-us/security/advisories/cve-2020-12803/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12803