Alerta de seguridad informática	9VSA-00063-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de octubre de 2019
Última revisión	08 de octubre de 2019

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 del sitio web oficial de Foxit, referente a vulnerabilidades detectadas en el lector de PDF Foxit para Windows, junto a su respectiva actualización para mitigar el riesgo.

Vulnerabilidades

- CVE-2019-5031
- CVE-2019-13123
- CVE-2019-13124
- CVE-2019-13326
- CVE-2019-13327
- CVE-2019-13328
- CVE-2019-13329
- CVE-2019-13330
- CVE-2019-13331
- CVE-2019-13332
- CVE-2019-17183

Impactos

CVE-2019-5031, CVE-2019-13123 y CVE-2019-13124: Aplicación expuesta a ejecución de código remoto y a caída por error inesperado de falta de memoria en el motor V8 al ejecutar un JavaScript especialmente diseñado.

CVE-2019-13326, CVE-2019-13327 y CVE-2019-13328: Vulnerabilidad de tipo ejecución de código remoto, la cual es gatillada por causa de cómo Foxit maneja los campos AcroForm (campos del PDF en los cuales el usuario puede ingresar datos).

CVE-2019-13329, CVE-2019-13330 y CVE-2019-13331: Vulnerabilidad de tipo ejecución de código remoto "type-confusion", al no manejar correctamente los archivos de tipo TIF y JPG.

CVE-2019-13332: Vulnerabilidad de tipo ejecución de código remoto en XFA Form Template (XML Form Architecture).

CVE-2019-17183: Aplicación expuesta a infracción de acceso y, por la condición de falta de memoria en el sistema actual, podría caerse al ser lanzada.

Producto Afectado

Foxit versión 9.6.0.25114 y anteriores.

Mitigación

Actualizar a la versión 9.7 de Foxit, se puede actualizar directamente apretando en la pestaña "Help" y luego en "Check for updates".

Enlaces

- https://www.foxitsoftware.com/downloads/#Foxit-Reader/
- https://www.foxitsoftware.com/support/security-bulletins.php
- https://nvd.nist.gov/vuln/detail/CVE-2019-5031
- https://nvd.nist.gov/vuln/detail/CVE-2019-13123
- https://nvd.nist.gov/vuln/detail/CVE-2019-13124
- https://nvd.nist.gov/vuln/detail/CVE-2019-13326
- https://nvd.nist.gov/vuln/detail/CVE-2019-13327
- https://nvd.nist.gov/vuln/detail/CVE-2019-13328
- https://nvd.nist.gov/vuln/detail/CVE-2019-13329
- https://nvd.nist.gov/vuln/detail/CVE-2019-13330
- https://nvd.nist.gov/vuln/detail/CVE-2019-13331
- https://nvd.nist.gov/vuln/detail/CVE-2019-13332
- https://nvd.nist.gov/vuln/detail/CVE-2019-17183

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.10.08 13:13:04 -03'00'