Alerta de seguridad informática	9VSA20-00125-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de enero de 2020
Última revisión	17 de enero 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 información obtenida de Foxit, referente a vulnerabilidades que afectan a Foxit Reader y PhantomPDF, las cuales de ser explotadas permitirían a un atacante remoto realizar ataques de corrupción de memoria comprometiendo al sistema vulnerable. Este informe incluye la respectiva mitigación.

Vulnerabilidades

CVE-2019-5130

CVE-2019-5145

CVE-2019-5131

CVE-2019-5126

Impacto

Un atacante podría realizar la ejecución de código remoto sobre el sistema Windows afectado debido a errores de corrupción en memoria al manejar incorrectamente marcas de agua, objetos AcroForm, cajas de texto u objetos JavaScript en archivos PDF. La explotación de esta vulnerabilidad permitiría a un atacante comprometer completamente al sistema afectado.

Productos Afectados

Para Foxit Reader, versiones anteriores a la 9.7.0.29478 (incluida).
Para PhantomPDF, versiones anteriores a la 9.7.0.29455 (incluida).

Mitigación

Actualizar a la versión 9.7.1 de Foxit Reader.
Actualizar a la versión 9.7.1 de PhantomPDF.

Enlaces

https://www.foxitsoftware.com/support/security-bulletins.php
https://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2019-5130
https://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2019-5145
https://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2019-5131
https://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2019-5126

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.01.17 06:59:14 -03'00'