

| | |
|---------------------------------|------------------------------|
| Alerta de seguridad cibernética | 9VSA20-00349-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 30 de diciembre de 2020 |
| Última revisión | 30 de diciembre 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 entregada por OpenJPEG sobre seis vulnerabilidades que afectan a la biblioteca de código abierto OpenJPEG.

Este informe incluye las medidas de mitigación, consistentes en instalar la última actualización de los productos afectados.

Vulnerabilidades

CVE-2020-15389
CVE-2020-27814
CVE-2020-27824
CVE-2020-27841
CVE-2020-27844
CVE-2020-27845

Impacto

Las seis vulnerabilidades son categorizadas como de riesgo alto. Esto porque permiten que un atacante remoto ejecute código arbitrario en el sistema objetivo, pudiendo comprometerlo completamente.

Productos Afectados

OpenJPEG 2.3.0 y 2.3.1.

Mitigación

Instalar las actualizaciones del sitio del desarrollador.

Enlaces

<https://github.com/uclouvain/openjpeg/releases/tag/v2.4.0>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15389>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27814>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27824>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27841>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27844>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27845>