Alerta de seguridad informática	9VSA-00109-001
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 2019
Última revisión	30 de diciembre 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 información obtenida de la fuente oficial de Apache, referente a una vulnerabilidad que afecta a Apache Solr, la cual, de ser explotada, permitiría a un atacante remoto ejecutar código en el contexto de la aplicación. El informe contiene la respectiva mitigación.

Vulnerabilidad

CVE-2019-17558

Impactos

Esta vulnerabilidad se debe a la falta de sanitización al ingresar datos en “VelocityResponserWriter”, cuando “params.resource.lodaer.enables” es definido como verdadero en las configuraciones de Apache Solr. Un usuario remoto autenticado, con la capacidad de subir templates o cambiar las configuraciones del programa, podría inyectar templates maliciosos o ejecutar códigos arbitrarios en el sistema afectado. Una explotación exitosa permitiría comprometer completamente al sistema.

Producto Afectado

Apache Solr entre las versiones 5.0.0 y 8.3.1 (incluidas).

Mitigación

Se debe actualizar a la versión 8.4 o aplicar los cambios necesarios en las configuraciones (para más información, visitar enlaces mencionados al final del documento).

Enlaces

https://issues.apache.org/jira/browse/SOLR-13971
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17558