Alerta de seguridad informática	9VSA20-00146-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Febrero de 2020
Última revisión	24 de Febrero 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 múltiples fuentes, referente a una vulnerabilidad que afecta al componente PyYAML de Python, la cual de ser explotada permitiría a un atacante obtener acceso a funciones restringidas. Este informe incluye la respectiva mitigación.

Vulnerabilidad

CVE-2019-20477

Impacto
Debido a una restricción de acceso deficiente en las funciones “load” y “load_all”, un atacante remoto podría evadir esta restricción de acceso y obtener acceso no autorizado a la aplicación.

Producto Afectado
PyYAML 5.1.

Mitigación
Actualizar a la versión 5.3.

Enlaces
https://www.cybersecurity-help.cz/vdb/SB2020022409
https://github.com/yaml/pyyaml/blob/master/CHANGES
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-20477