Alerta de seguridad cibernética	9VSA20-00274-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de julio de 2020
Última revisión	18 de julio 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 obtenida de Python respecto a vulnerabilidad de tipo denegación de servicios que le afecta. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidad

CVE-2020-14422

CVE-2020-14422

Una vulnerabilidad de tipo colisión de hashes en IPv4 e IPv6 podría convertirse en una denegación de servicios, esto debido a la forma en que interactúan IPv4Interface e IPv6Interface, que siempre devuelven 32 y 64 respectivamente. Si uno de los objetos es puesto en un diccionario, por ejemplo un servidor que guarda IPs, esto causará una colisión de hashes lo cual se convertirá en una denegación de servicios.

Productos Afectados

Python desde la versión 3.8.0 hasta la 3.8.3.

Mitigaciones

Actualizar a la versión 3.8.4 de Python.

Enlaces

https://bugs.python.org/issue41004
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14422