Alerta de seguridad informática	9VSA20-00121-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de enero de 2020
Última revisión	14 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 Nginx, referente a una vulnerabilidad que afecta a su servidor web/proxy/mail, la cual de ser explotada permitiría a un atacante remoto obtener acceso a páginas web no autorizadas. Este informe incluye la respectiva mitigación.

Vulnerabilidad

CVE-2019-20372

Impacto

Ciertas configuraciones en error_page permitirían a un atacante leer páginas web no autorizadas en entornos en los que Nginx está frente al balanceador de carga, esto debido a que el servidor no maneja bien las peticiones HTTP, permitiendo una vulnerabilidad de tipo “HTTP request Smuggling”.

Productos Afectados

Todas las versiones de Nginx desde la 1.17.0 hasta la 1.17.6.

Mitigación

Se debe actualizar a la versión 1.17.7 de Nginx.

Enlaces

http://nginx.org/en/CHANGES
https://www.cybersecurity-help.cz/vdb/SB2020011323
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-20372