Alerta de seguridad cibernética	9VSA20-00167-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de abril de 2020
Última revisión	01 de abril 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 ElasticStack referente a una vulnerabilidad que afecta a su moto de base de datos y búsquedas, la cual permite la escalación de privilegios en el sistema afectado. Este informe incluye la respectiva mitigación.

VULNERABILIDAD

CVE-2020-7009

CVE-2020-7009

Impacto
Debido a un error de permisos inapropiados en el motor de búsquedas y base de datos, un atacante remoto capaz de generar una llave API podría realizar una serie de pasos para lograr que esa llave se genere con privilegios elevados.

Productos Afectados
Elasticseach desde la versión 6.7.0 hasta la 6.8.7 y desde la versión 7.0.0 hasta la 7.6.1.

Mitigación
Se debe actualizar a Elasticsearch versión 7.6.2 o versión 6.8.8.

Enlaces
https://discuss.elastic.co/t/elastic-stack-6-8-8-and-7-6-2-security-update/225920
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7009