Alerta de seguridad cibernética	9VSA21-00392-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de febrero de 2021
Última revisión	17 de febrero de 2021

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 sobre una vulnerabilidad que afecta Ignition para Laravel.

Este informe incluye las medidas de mitigación, consistentes en instalar la última actualización de los productos afectados.

Vulnerabilidad

CVE-2021-3129

Impacto

CVE-2021-3129 permite a un atacante remoto ejecutar código arbitrario en el sistema objetivo. La vulnerabilidad existe debido a una validación inapropiada de los datos ingresados en Ignition. Un atacante remoto puede enviar una solicitud especialmente diseñada a la aplicación y leer o escribir archivos arbitrarios en el sistema.

La vulnerabilidad puede ser explotada por un atacante remoto no autenticado, a través de internet.

Productos Afectados

Ignition, versiones 1.16.0 a 1.16.4

Mitigación

Instalar las respectivas actualizaciones desde el sitio del proveedor.

Enlaces

https://www.ambionics.io/blog/laravel-debug-rce

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3129

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.02.17 17:57:17 -03'00'