Alerta de seguridad cibernética	9VSA20-00215-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de mayo de 2020
Última revisión	15 de mayo 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 ClamAV referente a dos vulnerabilidades que afectan a su AntiVirus. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidades

CVE-2020-3341
CVE-2020-3327

CVE-2020-3341

Debido a una condición de límites con las rutinas de desencriptación AES al procesar archivos PDF en el AV, un atacante podría crear un archivo PDF especialmente diseñado, entregárselo a la aplicación y causar una denegación de servicios.

Producto Afectado
ClamAV versión 0.102.2.

Mitigación
Actualizar a la versión 0.102.3 de ClamAV.

Enlaces
https://blog.clamav.net/2020/05/clamav-01023-security-patch-released.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3341

CVE-2020-3327

Debido a un error en memoria al procesar archivos ARJ, un atacante podría crear archivos ARJ especialmente diseñados para gatillar el error y causar una denegación de servicios

Productos Afectados
ClamAV versiones 0.101 hasta 0.102.2.

Mitigación
Actualizar a la versión 0.102.3 de ClamAV.

Enlaces
https://blog.clamav.net/2020/05/clamav-01023-security-patch-released.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3327