

Alerta de seguridad cibernética	9VSA20-00255-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de junio de 2020
Última revisión	26 de junio 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 afectada a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información obtenida del Laboratorio ECE/CIS de la Universidad de Delaware referente a vulnerabilidad que afecta al protocolo NTP (Network Time Protocol). El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidad

CWE-401

CWE-401

Por cada paquete enviado entre los demonios NTP, se liberará una pequeña porción de memoria, y eventualmente estos se quedarán sin suficiente memoria, causando una denegación de servicios.
Impacto: medio.

Productos Afectados

Asociados que usen autenticación CMAC a través de los ntpd entre las versiones 4.2.8p11/4.3.97 y 4.2.8p14/4.3.100.

Mitigación

Actualizar a la versión 4.2.8p15 de NTP.

Enlaces

https://www.eecis.udel.edu/~ntp/ntp_spool/ntp4/NEWS