Alerta de seguridad informática	**9VSA-00025-001**
Clase de alerta	**Vulnerabilidad**
Tipo de incidente	**Sistema y/o Software Abierto**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**29 de Julio de 2019**
Última revisión	**29 de Julio de 2019**

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 entregada por la empresa Wind River acerca de vulnerabilidades que afectan a su producto VxWorks

Vulnerabilidad

- CVE-2019-12256
- CVE-2019-12257
- CVE-2019-12255
- CVE-2019-12260
- CVE-2019-12261
- CVE-2019-12263
- CVE-2019-12258
- CVE-2019-12259
- CVE-2019-12262
- CVE-2019-12264
- CVE-2019-12265

Impacto

CVE-2019-12256
Un paquete IPv4 especialmente diseñado, que contiene opciones SSRR / LSRR codificadas no válidas, puede causar un desbordamiento de la pila de llamadas. No se requieren servicios específicos más allá del soporte del protocolo IPv4.

CVE-2019-12257
Un paquete DHCP especialmente diseñado puede causar un desbordamiento de memoria en el sistema VxWorks usando DHCP. El atacante debe compartir la LAN con el dispositivo ya que los enrutadores IP no reenvían los paquetes DHCP.

CVE-2019-12255
Un segmento TCP especialmente diseñado con el conjunto de indicadores URG puede provocar un desbordamiento del búfer pasado a las rutinas de socket recv(), recvfrom() o recvmsg().

CVE-2019-12260
Una serie de segmentos TCP especialmente diseñados donde el último paso es un segmento TCP con el conjunto de indicadores URG puede provocar un desbordamiento del búfer pasado a las rutinas de socket recv (), recvfrom () o recvmsg ().

CVE-2019-12261
Como respuesta, se envía una respuesta especialmente diseñada al intento de conexión, donde también se establecen los indicadores FIN y URG. Esto puede poner a la víctima en un estado inconsistente, lo que hace posible enviar otro segmento que desencadena un desbordamiento del búfer.

CVE-2019-12263
Vulnerabilidad de seguridad de IPNET: confusión del estado del puntero urgente TCP debido a la condición de carrera

CVE-2019-12258
Un paquete especialmente diseñado que contiene opciones TCP ilegales puede hacer que la víctima no solo abandone el segmento TCP sino que también elimine la sesión TCP.

CVE-2019-12259
DoS a través de la anulación de referencia NULL en el análisis IGMP. Esta vulnerabilidad requiere que a la pila TCP / IP se le asigne una dirección de multidifusión, la API para la asignación de direcciones de unidifusión o algo con la misma falla lógica es un requisito previo.

CVE-2019-12262
El manejador de recepción RARP verifica que el paquete esté bien formado, pero no puede verificar que el nodo tenga una transacción RARP en curso que coincida con el paquete recibido.

CVE-2019-12264
El cliente DHCP de VxWorks no puede validar correctamente que la dirección IP ofrecida en una renovación de DHCP u respuesta de oferta contenga una dirección de unidifusión válida. Un atacante puede asignar direcciones de difusión o multidifusión a la víctima.

CVE-2019-12265
Un atacante puede crear un informe de consulta IGMPv3 especialmente diseñado y fragmentado, lo que puede provocar que la víctima transmita contenido de búfer indefinido.

Mitigación

Se recomienda realizar las actualizaciones según lo indicado por el fabricante.

Enlace

https://support2.windriver.com/index.php?page=cve&on=view&id=CVE-2019-12257
https://support2.windriver.com/index.php?page=cve&on=view&id=CVE-2019-12256
https://support2.windriver.com/index.php?page=cve&on=view&id=CVE-2019-12255
https://support2.windriver.com/index.php?page=cve&on=view&id=CVE-2019-12260
https://support2.windriver.com/index.php?page=cve&on=view&id=CVE-2019-12261
https://support2.windriver.com/index.php?page=cve&on=view&id=CVE-2019-12263
https://support2.windriver.com/index.php?page=cve&on=view&id=CVE-2019-12258
https://support2.windriver.com/index.php?page=cve&on=view&id=CVE-2019-12259
https://support2.windriver.com/index.php?page=cve&on=view&id=CVE-2019-12262
https://support2.windriver.com/index.php?page=cve&on=view&id=CVE-2019-12264
https://support2.windriver.com/index.php?page=cve&on=view&id=CVE-2019-12265

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.07.30 18:52:05 -04'00'