# VULNERABILIDAD EN 499ES ETHERNET/IP STACK DE RTA

BCSC_ALERTA_VULNERABILIDAD_RTA's_499ES_ENIP_STACK

TLP:WHITE

www.basquecybersecurity.eus

Noviembre 2020

# TABLA DE CONTENIDO



## Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de BCSC como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de BCSC. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

## Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

## SOBRE EL BCSC

El Centro Vasco de Ciberseguridad (Basque Cybersecurity Centre, BCSC) es la entidad designada por el Gobierno Vasco para elevar el nivel de madurez de la ciberseguridad en Euskadi.

Es una iniciativa transversal que se enmarca en la Agencia Vasca de Desarrollo Empresarial (SPRI), sociedad dependiente del Departamento de Desarrollo Económico e Infraestructuras del Gobierno Vasco. Así mismo, involucra a otros tres Departamentos del Gobierno Vasco: el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación, y a cuatro agentes de la Red Vasca de Ciencia, Tecnología e Innovación: Tecnalia, Vicomtech, Ikerlan y BCAM.


El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución de proyectos de colaboración entre actores complementarios en los ámbitos de innovación tecnológica, investigación y transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

Así mismo, ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CERT, por sus siglas en inglés “Computer Emergency Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca. Con el fin de alcanzar estos objetivos forma parte de diferentes iniciativas orientadas a la gestión de incidentes de ciberseguridad:

# RESUMEN EJECUTIVO

Investigadores de seguridad han reportado la existencia de una **vulnerabilidad crítica** en las implementaciones de **499ES EtherNet/IP (ENIP) stack** desarrollado por **Real Time Automation (RTA)**, presentes en multitud de dispositivos de automatización industrial.

La vulnerabilidad **CVE-2020-25159** está basada en un desbordamiento de buffer que podría permitir a un atacante remoto no autenticado causar una condición de denegación de servicio (**DoS**) y llevar a cabo la ejecución de código (**RCE**).

De forma concreta, el fallo reside en todas las **versiones anteriores a la 2.28**, sin incluir, del código fuente de la región stack de EtherNet/IP (ENIP), sustituido por Real Time Automation en 2012, aunque se estima que aún se continúa utilizando en múltiples firmwares de terceros. Según los investigadores, más de 8.000 dispositivos conectados a Internet son compatibles con ENIP.

Para solucionar la vulnerabilidad, es necesario **actualizar** a la última versión disponible del producto afectado poniéndose en contacto con el equipo de Real Time Automation.

# ANÁLISIS TÉCNICO

El código fuente del stack de la memoria de **499ES EtherNet/IP (ENIP)**, desarrollado por Real Time Automation (RTA) y empleado en multitud de dispositivos de automatización industrial, contiene una vulnerabilidad que podría exponer a un amplio número de industrias a ataques remotos.

EL protocolo de red EtherNet/IP (**ENIP**), basado en el estándar de Control e Información (CIP), es ampliamente utilizado en aplicaciones de automatización industrial para garantizar la correcta comunicación en tiempo real entre dispositivos. El problema reside en que existen multitud de fabricantes que incorporan a sus dispositivos implementaciones de este protocolo desarrolladas por terceros, en este caso, se trata de una implementación desarrollada por Real Time Automation, concretamente, las versiones de 499ES EtherNet/IP (ENIP) anteriores a 2012.

Referenciada como **CVE-2020-25159**, la vulnerabilidad podría causar una condición de denegación de servicio (**DoS**) y un desbordamiento de buffer que podría permitir la ejecución de código de forma remota (**RCE**) en los dispositivos que ejecutan una implementación de EtherNet/IP de RTA vulnerable.

El fallo está ocasionado por un intento de reducción del uso de RAM por parte del fabricante mediante la limitación del tamaño del buffer usado en las **solicitudes EtherNet/IP Forward Open**. La limitación de RAM podría permitir a un atacante sobrepasar el buffer destinado y, posteriormente, realizar modificaciones no autorizadas. Para ello, un atacante tendría que enviar una solicitud Forward Open especialmente diseñada a través del puerto TCP 44818 a un dispositivo expuesto en la red, necesario para establecer la comunicación entre el cliente y el punto final mediante una misma sesión CIP. El error se debe a una verificación de tamaño incorrecta de la ruta CIP de la conexión, que permitiría a un posible atacante escribir en una dirección de la memoria fuera del buffer de longitud fija destinado para ello, lo que derivaría en una interrupción del servicio (DoS) y, con los suficientes esfuerzos, podría permitir la ejecución de código (RCE).

```
int i = 0;
connection_struct.path_size = request->payload[parse_index];

while (i < connection_struct.path_size) {
    // Stack Overflow: 'path' has size of 32 values, but we can write up to
255 values
    connection_struct.path[i] = ReadWord(request->payload + parse_index);
    parse_index +=2;
    i++;
}
```

*Ilustración 1 Código similar al requerido para la explotación del fallo expuesto por los investigadores de seguridad que detectaron la vulnerabilidad*

La vulnerabilidad ha recibido un score de **9.8** en base a la escala **CVSSv3**, ya que permite la explotación de forma remota, con una complejidad baja, no es requerida autenticación alguna por parte del atacante, ni tampoco es necesaria la interacción del usuario, y un ataque exitoso supondría un impacto completo en la confidencialidad, integridad y disponibilidad del sistema. Por el momento, no se tiene constancia de reportes de actividad maliciosa en la red relacionada con este fallo, ni de la existencia de exploit o prueba de concepto públicamente disponibles.

Se encuentran afectados todos los dispositivos que ejecutan una **versión** del código fuente de la región stack de 499ES EtherNet/IP (ENIP) **anterior a la 2.28**, versión que no se encuentra afectada y que fue lanzada por Real Time Automation en **2012**. Si bien, aunque hace años que RTA solucionó el fallo, existen multitud de dispositivos que aún tienen implementada una versión vulnerable en su firmware. Según los hallazgos de los investigadores que reportaron la vulnerabilidad, al menos 11 dispositivos de 6 proveedores diferentes utilizan una versión vulnerable ENIP.

## MITIGACIÓN / SOLUCIÓN

Para solucionar la vulnerabilidad, es necesario **actualizar a la última versión estable** del código fuente implementado en el stack de 499ES EtherNet/IP (ENIP). En este sentido, Real Time Automation ha instado a los usuarios y proveedores de control industrial a ponerse en contacto con su equipo de ingeniería a través del teléfono indicado, 800-249-1612, para **comprobar** si ejecutan una implementación ENIP vulnerable y, en su caso, ofrecer las pautas para **llevar a cabo la actualización**.

Por su parte, la Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA) ha realizado un aviso de seguridad en el que advierte sobre este fallo, para lo que incluye una serie de medidas de mitigación que se describen en lo sucesivo:

- Minimizar la exposición de todos los dispositivos y/o sistemas de control a la red y asegurar que no sean accesibles desde Internet.
- Localizar las redes de sistemas de control y los dispositivos remotos detrás de firewall y aislarlos de la red de la organización.
- Cuando se requiera el acceso remoto, utilizar métodos seguros, tales como redes privadas virtuales (VPN), teniendo en cuenta que las VPN pueden tener vulnerabilidades y deben estar actualizadas a la versión más reciente disponible.

## REFERENCIAS ADICIONALES

- Lingering RTA ENIP stack vulnerability poses risk to ICS devices
- ICS Advisory (ICSA-20-324-03) - Real Time Automation EtherNet/IP
- Secure EtherNet/IP Devices


## Reportar incidente

Si has detectado algún incidente de ciberseguridad, avísanos para que tomemos las medidas oportunas para evitar su propagación.

900 104 891

incidencias@bcsc.eus

## Catálogo de ciberseguridad

¿Necesitas ayuda con tu ciberseguridad o la de tu empresa?