ALIAS ROBOTICS
Robot Cybersecurity

# Alias Robotics descubre numerosas (y peligrosas) vulnerabilidades en las comunicaciones del Sistema Operativo de Robots (ROS) que pueden tener *"devastadoras consecuencias de seguridad"*

- **La firma vitoriana de ciberseguridad robótica lidera una vez más una investigación que involucra expertos internacionales sobre la importancia de la seguridad en el Sistema Operativo de Robots (ROS) y el protocolo de comunicaciones DDS**
- **Los participantes en el estudio han descubierto casi una quincena de peligrosas vulnerabilidades presentes en más de 650 dispositivos, muy habituales en el ámbito Industrial, la Universidad, e incluso en Hospitales y Agencias Militares**
- **La investigación de Alias Robotics ha sido citada y publicada por la Agencia de Seguridad e Infraestructuras de Ciberseguridad de Estados Unidos lo cual refleja la importancia de las conclusiones expuestas**
- **Para mitigar estas vulnerabilidades, Alias Robotics ha contribuido con SROS2, una serie de herramientas para detectar inseguridades en ROS**

**Un equipo de investigadores liderado por la firma española Alias Robotics - especializada en ciberseguridad robótica- junto con expertos en ciberseguridad de varias multinacionales y responsables de ciberseguridad de varios gobiernos, han descubierto cerca de una quincena de peligrosas vulnerabilidades, algunas críticas, en el Sistema Operativo de Robots (ROS, en sus siglas en inglés) y los protocolos de comunicaciones DDS que afectan a los sistemas y robots industriales y, vulnerabilidades que de ser utilizadas por cibercriminales, podrían tener *"devastadoras consecuencias"*. A su vez, han detectado que estas vulnerabilidades están presentes en casi 650 dispositivos diferentes expuestos en Internet y utilizados no solo en la industria, sino en el campo de la salud o en ámbitos militares.**

Profesionales de seguridad robótica e informática de la firma alavesa Alias Robotics han colaborado en los últimos meses junto a expertos en tecnologías de la información de todo el mundo en la detección de **vulnerabilidades de seguridad en el Sistema Operativo de Robots (ROS) y en el software de comunicaciones DDS** ("Data Distribution Service" o Servicio de Distribución de Datos, en sus siglas en inglés), presentes en multitud de

sistemas (coches autónomos, brazos robóticos industriales, sistemas aeroespaciales, equipamientos militares, infraestructuras críticas, ...), además de en robots industriales.

En particular, las vulnerabilidades afectan a DDS, un 'software intermedio' (denominado middleware) que es el principal bus de comunicaciones entre diferentes dispositivos robóticos, es decir, **el núcleo de ROS (Robot Operating System), que usan la mayoría de ingenieras e ingenieros de robótica para todo tipo de robots industriales presentes o futuros**, con aplicaciones en el mundo empresarial, en el ámbito industrial, pero también en el mundo de la salud, como es el caso de los robots quirúrgicos. Un estudio independiente[1] apunta a que el uso de ROS crecerá significativamente durante los próximos años y que en el 2024 el 55% de los robots comercializados utilizarán ROS.

Desde Alias Robotics -especializada en ciberseguridad robótica- se considera que "*DDS* ***es un middleware de comunicaciones todavía ampliamente inseguro****, que se utiliza en áreas donde la seguridad es muy importante,* ***por lo que hace falta inversión en ciberseguridad de forma inmediata****".* Consideran, además, que los tiempos de respuesta de los fabricantes de DDS son largos, *"lo cual expone mucho estos sistemas a ciberataques",* según denuncia Víctor Mayoral-Vilches, investigador líder por parte de Alias Robotics y fundador de la 'startup' vitoriana.

A su juicio, ***"cibercriminales podrían a día de hoy utilizar estas vulnerabilidades para paralizar robots e infraestructuras críticas por todo el mundo",*** recalca Víctor Mayoral-Vilches. Desde la compañía vitoriana se alerta que es necesario que las empresas de robótica y de automatización inviertan en ciberseguridad y cooperen *"con grupos cualificados en la ciberseguridad robótica"*,

## Primeras claves

Los resultados de esta investigación son el fruto de la colaboración de varios investigadores que incluyen a Víctor Mayoral-Vilches (Alias Robotics), Federico Maggi, Mars Cheng, Patrick Kuo, Chizuru Toyama, Rainer Vosseler, y Ta-Lun Yen (Trend Micro y TxOne) y Erik Boasson (ADLINK Labs).

Su impacto en la robótica ha sido liderado por Alias Robotics y las claves **no son nada halagüeñas**. Es más, las investigaciones han sido calificadas como *"devastadores"* por las consecuencias que podrían tener en caso de utilización delictiva por parte de hackers informáticos, dado que buena parte de estas vulnerabilidades "***solo han sido parcheadas o***

[1] https://www.businesswire.com/news/home/20190516005135/en/Rise-ROS-55-total-commercial-robots-shipped

***mitigadas por los fabricantes",*** según denuncian los autores del trabajo de investigación.

Así, en un primer momento, el equipo liderado por Alias Robotics **ha llegado a detectar hasta 13 vulnerabilidades** de seguridad (algunas calificadas como *"críticas"* por expertos en ciberseguridad), que podrían afectar tanto a trabajadores y usuarios que manejan los robots industriales que incluyen este software DDS. No se descarta, sin embargo, la aparición de nuevas vulnerabilidades en los próximos meses, según se profundice en el estudio.

Una de las conclusiones es que estas vulnerabilidades **están presentes en casi 650 diferentes dispositivos robóticos utilizados en todos los campos económicos** de todo el mundo. Desde Alias Robotics han detectado dispositivos afectados por estas vulnerabilidades en organizaciones como la NASA, pero también en centros mundiales de datos (Huawei Cloud Service), grandes multinacionales industriales (Siemens), así como hospitales, bancos y universidades de 34 países, afectando a 100 organizaciones a través de 89 proveedores de servicios de Internet (ISP).

## Principales vulnerabilidades

Estas vulnerabilidades detectadas podrían llegar a suponer **la pérdida de control del dispositivo robótico**, la pérdida de seguridad del mismo, la denegación de servicios mediante la fuerza bruta, la posibilidad de facilitar el acceso al dispositivo mediante la explotación de servicios remotos, o bien problemas en la cadena de suministro o el que los atacantes abusen de los propios de protocolos de seguridad para crear un canal de mando y control eficiente.

Los autores del estudio, y pese a la insistencia en los últimos meses para su corrección y subsanación, han constatado que muchas de estas vulnerabilidades de seguridad -algunas incluso con el código fuente (propietario) expuesto a todo el público- han estado abiertas ***"por mucho tiempo, incluso años, por lo que cibercriminales podrían a día de hoy utilizarlas para paralizar infraestructuras críticas de todo el mundo",*** según denuncia Víctor Mayoral-Vilches,

A su juicio, **"todavía muchos *fabricantes de dispositivos robóticos priorizan el desarrollo de su negocio y continúan ignorando la ciberseguridad*".** Mayoral-Vilches hace hincapié en que muchos de los fabricantes se niegan a solucionar los problemas "*porque si lo hicieran incumplirían la norma/especificación de DDS*". "*Este es un problema de magnitud* -recalca el fundador de Alias Robotics- *ya que la revisión de la norma de DDS puede tardar años en ser revisada de forma apropiada*".

El informe, **que ha sido recientemente citado y publicado por la Agencia de Seguridad e Infraestructuras de Ciberseguridad de Estados Unidos,** fue presentado durante 2021 en varios foros incluyendo el 'Black

Hat 2021' de Las Vegas, el mayor foro anual de ciberseguridad del mundo- , pero también en la ROS-Industrial Conference 2021 y más recientemente en una sesión organizada por la Comisión Europea. Su investigación continuará siendo presentada durante este 2022 en nuevas conferencias y foros industriales.

## Herramientas para identificar vulnerabilidades de ROS 2 y DDS

A fin de mitigar las amenazas encontradas y capacitar a ingenieros de robótica en materia de seguridad, el equipo de Alias Robotics ha liderado un segundo esfuerzo de investigación que ha producido y liberado con licencia de código abierto una serie de herramientas que permiten detectar estas vulnerabilidades en ROS 2 y DDS.

Los resultados de este esfuerzo han sido resumidos en el artículo "SROS2: Usable Cyber Security Tools for ROS 2" que ha sido enviado a la Conferencia Internacional de Robots y Sistemas (IROS 2022), uno de los eventos más relevantes cada año en el sector de la robótica y que se dará cita en Kioto (Japón) el próximo 23 de octubre.

ALIAS ROBOTICS
Robot Cybersecurity

**Alias Robotics** se fundó en 2018 por Víctor Mayoral-Vilches y se ha convertido en un líder internacional en soluciones de ciberseguridad para robots. Su equipo es el creador del primer Robot Immune System (RIS), un antivirus inteligente que protege a los robots de los ciberdelincuentes desde adentro hacia afuera. RIS se incorpora a los robots para protegerlos a medida que evoluciona y se adapta como el sistema inmunológico humano.

Alias Robotics está integrada por reconocidos ingenieros en robótica, científicos e investigadores de seguridad con una experiencia de más de 10 años. Entre sus clientes se incluyen grandes empresas de automatización, instituciones gubernamentales y usuarios de robots industriales www.aliasrobotics.com


- Comunicación:

Gontzal Sáenz — ieR-Información en Red
Tlfno: 646 77 68 08
e-mail: gsaenz@informacionenred.com