Nuclear Regulatory Commission

Chief Information Security Officer

On November 11, 2021 the Department of Homeland Security Cybersecurity and Infrastructure Security Agency released an Industrial Control Systems Cyber Emergency Readiness Team Advisory ICSA-21-315-02 for Multiple Data Distribution Services (DDS) implementations.

The attached advisory details vulnerabilities found in multiple Object Management Group DDS implementations with the following products:

- Eclipse CycloneDDS: All versions prior to 0.8.0
- eProsima Fast DDS: All versions prior to 2.4.0 (#2269)
- GurumNetworks GurumDDS: All versions
- Object Computing, Inc. (OCI) OpenDDS: All versions prior to 3.18.1
- Real-Time Innovations (RTI) Connext DDS Professional and Connext DDS Secure: Versions 4.2x to 6.1.0
- RTI Connext DDS Micro: Versions 3.0.0 and later
- TwinOaks Computing CoreDX DDS: All versions prior to 5.9.1

It is the responsibility of your organization to review its systems and inventory for the implementation of any of these affected products. Accordingly, the following must be reported to the Nuclear Regulatory Commission (NRC) Chief Information Security Officer (CISO) by December 31, 2021:

- any impacted system(s) and remediation actions you have or plan to implement;
- any system where you are unable to remediate an identified vulnerability; or,
- if applicable, verify there are no instances of any of these impacted products within your environment

Failure to report impacted systems or to implement corrective actions may result in an increase of risk to your systems. The NRC CISO and representatives are available to assist in identifying vulnerabilities and potential corrective actions. Please feel free to contact the NRC CISO at CISO@nrc.gov if you have questions or concerns.

Thank you,

Jonathan Feibus
Chief Information Security Officer
U.S. Nuclear Regulatory Commission
Office of the Chief Information Officer
11545 Rockville Pike, Rockville, MD 20850
Office: 301-415-0717 | TWFN 6B85