ANALYZING THE DATA DISTRIBUTION SERVICE (DDS) PROTOCOL FOR CRITICAL INDUSTRIES

Even among industry practitioners themselves, little is known about the Data Distribution Service (DDS) protocol, a middleware technology in use for more than a decade by critical industries as a machine-to-machine communication layer. This software is responsible for driving billions of devices and mechanisms every day, and usage is steadily increasing as it responds to applications' and embedded systems' real-time requirements. Our research, "A Security Analysis of the Data Distribution Service (DDS) Protocol" looked into the standard's security posture and ecosystem as a critical software component of various industrial sectors.

DDS use in industries, its vulnerabilities, and the potential impact of compromise

As DDS is located at the beginning of the supply chain, it is easy to lose track of and an ideal attack target. Here is a list of industries that make use of DDS, new vulnerabilities we found, the types of potential attacks that malicious actors can do when the security gaps are abused, and the impact on these sectors when compromised.

Sectors	New vulnerabilities	Potential attacks and impact
• Telecommunications and networks • Defense • Virtualization and cloud • Energy • Healthcare • Mining • Industrial internet of things (IIoT) and robotics • Public and private transportation	• CVE-2021-38425 • CVE-2021-38429 • CVE-2021-38487 • CVE-2021-43547 • CVE-2021-38447 • CVE-2021-38445 • CVE-2021-38423 • CVE-2021-38435 • CVE-2021-38439 • CVE-2021-38427 • CVE-2021-38433 • CVE-2021-38443 • CVE-2021-38441	Potential attacks ◦ Spoofing ◦ Reconnaissance ◦ Automated data collection ◦ Denial of service (DoS) • Compromise on the network attack surface: Loss of control on affected system • Compromise on the developer or system integrator: Loss of software supply chain integrity

Conclusion and mitigation practices

A look at the industries utilizing this technology reveal instances in which patches or remediations for DDS security gaps will not always be possible, easy, or available. In the short term, enterprises and users of DDS are advised never to expose endpoints unless necessary and equipped with the security measures for every instance of exposure. In the long term, companies should consider the implementation of supply chain management processes for critical components such as DDS libraries and ensure that these technologies are constantly monitored and tested.

Read the full research paper at https://research.trendmicro.com/ddsprotocol for more on the DDS protocol and how defend against threats that target it.

TREND MICRO | research