

Festo Products Considered Critical Infrastructure by the Cybersecurity & Infrastructure Security Agency

Rapid dissemination of security advisories for connected products is core to Festo's cybersecurity efforts.

The Cybersecurity & Infrastructure Security Agency (CISA), America's cyber defense agency, now includes Festo cybersecurity advisories on its website (www.cisa.gov). The CISA website is the authoritative source of vulnerability and remediation information in the United States and is a place where the leading connected products suppliers seek to post their security advisories.

Festo's cybersecurity journey began in 2020 with the formation of the Product Security Incident Response Team (PSIRT). The company slowly grew the infrastructure for developing and maintaining secure products. Festo formed the Central Department of Product Security in early 2023, when Florian Fetz, Head of Software Processes, Methods, and Tools, joined the company. Fetz began building the Central Department's team.

The Central Department implements and maintains processes and policies for product development with a focus on product security. The department is also responsible for tracking and communicating product vulnerabilities.

"Festo connected products were developed in line with state-of-the-art technology," said Tobias Pfeiffer, Global Product Security Officer. "The company recognizes that it is impossible to predict every vulnerability that can occur over a product's lifecycle and that is where the PSIRT takes over."

"PSIRT is the first point of contact when vulnerabilities are discovered, and the information is relayed to Festo," said Aleg Vilinski, Head of Product Security. "The PSIRT team analyzes the level of risk in the vulnerability, develops remediation solutions, and publishes comprehensive advisories listing product identification, the issue, and the solution(s) on the Festo [advisory webpage in its support portal](#) and with third parties like CISA (<https://www.cisa.gov/news-events/cybersecurity-advisories>) and CERT@VDE (<https://certvde.com/en/advisories/>)."

Vilinski continued, "Over the past year, Festo demonstrated the critical infrastructure position of its products by documenting for CISA personnel the range and type of Festo connected products used in the manufacturing, food and beverage, and processing industries, the number of Festo product installations in North America, and the central position these products play in automated systems."

Festo is certified to IEC 62443-4-1, the first international standard for the cybersecurity of industrial automation and control systems. By 2027, Festo connected products will be compliant with the European Union's Cyber Resilience Act (CRA). These CRA compliant products will feature:

- Secure development practices, including secure coding practices

09. July 2025

Responsible
according to press
law:
Christian Österle



Download/View press
release and press
images.

- Vulnerability management, including regular scanning and patching to address security issues
- Software Bill of Materials (SBOM) information that enables better identification of potential vulnerabilities. ([Festo offers an open-source tool for SBOM.](#))
- Incident reporting of critical security incidents to relevant authorities
- User friendly security features, including clear guidance on how to use security features
- CE marking showing the product meets CRA standards

Festo summarizes its approach to security in its [Security white paper for Festo controllers](#). The work of PSIRT is detailed on the Festo [PSIRT webpage](#), which includes secure contact information for those reporting vulnerabilities.

For more information on the advantages of working within the Festo ecosystem of less engineering overhead, fast time to market, seamless connectivity, and the industry's widest selection of electric and pneumatic automation components, visit www.festo.com.

Immagini stampa

