"Critical Vulnerabilities Identified in CODESYS ICS Automation Software"

Submitted by grigby1 on Fri, 06/04/2021 - 11:51am

Researchers from Positive Technologies have identified ten vulnerabilities in CODESYS automation software for Industrial Control Systems (ICS), some of which have been rated high and critical in severity. According to Vladimir Nazarov, Head of ICS Security at Positive Technologies, the exploitation of these vulnerabilities can lead to remote command execution on a Programmable Logic Controller (PLC), which may, in turn, disrupt technological processes, cause industrial accidents, and create significant economic losses. Attackers do not need a username or password to exploit the vulnerabilities. Having access to the industrial would suffice. The researchers say that the main root of the vulnerabilities is insufficient input data verification, which could be the cause of failed compliance with secure development recommendations. Companies are advised to follow recommendations provided in CODESYS official notices to eliminate the vulnerabilities. This article continues to discuss the severity, potential exploitation, and elimination of the vulnerabilities found in CODESYS ICS automation software.

Help Net Security reports "Critical Vulnerabilities Identified in CODESYS ICS Automation Software"