SB 26-02

JULY 2026

Transit Cybersecurity Events

Purpose

The Federal Transit Administration (FTA) is issuing this Safety Bulletin to raise awareness of a cybersecurity advisory from the Cybersecurity and Infrastructure Security Agency (CISA). FTA encourages transit agencies to review the information, assess whether it applies to their systems, and take the necessary steps to mitigate potential vulnerabilities. CISA's Cybersecurity Advisory can be found here – https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a.

Background

Agencies must remain vigilant against cybersecurity threats. Both state actors and non-state actors present a persistent risk to U.S. critical infrastructure, including public transit systems. Recent cybersecurity attacks on transit agencies highlight the need for transit agencies to continually assess vulnerabilities and update response and recovery plans to address evolving threats.

CISA, the Federal Bureau of Investigation (FBI), and several other co-authoring federal agencies issued a joint Cybersecurity Advisory: *Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers (PLCs) Across U.S. Critical Infrastructure.*

FTA encourages public transit agencies to review the full advisory that details how advanced persistent threat actors are targeting internet-facing operational technology devices. For more information related to cybersecurity readiness, please visit FTA's Cybersecurity Resources for Transit Agencies.

Summary of CISA's Cybersecurity Advisory

The CISA Cybersecurity Advisory identifies affected products, including Rockwell Automation/Allen-Bradley PLCs (such as CompactLogix and Micro850), and notes that actors may also be targeting devices manufactured by other companies, such as the Siemens S7 PLC.

The advisory outlines indicators of compromise to assist security teams in hunting for malicious activity and provides actionable mitigations, such as the following immediate steps and related resources, to prevent the attack:

1. Disconnect the PLC from the public-facing internet.
2. For controllers with a physical mode switch, place the physical mode switch into run position to prevent remote modification.
3. For devices that allow for software key switching, enable programming protection in PLC configuration software to limit who can modify PLCs remotely.
4. Create and test strong backups of the logic and configurations of PLCs.

The advisory includes additional resources and information on how to enroll in no-cost scanning to help organizations review their internet-accessible assets and reduce their threat exposure. Entities interested in enrolling in CISA's Cyber Hygiene Services can find more information on the offerings and enrollment process from CISA's website: Cyber Hygiene Services | CISA.

U.S. organizations are encouraged to report suspicious or criminal activity related to information in this advisory to CISA (contact@cisa.dhs.gov | or 1-844-Say-CISA (1-844-729-2472), the FBI (Field Offices — FBI), and/or the NSA (CybersecurityReports@nsa.gov).