(TLP:CLEAR) Joint Cybersecurity Advisory – Active Targeting of Siemens S7 PLCs

TLP:CLEAR

Author: Chase Snow
Created: Thursday, August 20, 2026 - 9:55
Categories: Cybersecurity, Federal & State Resources, OT-ICS Security

Summary: Yesterday, the NSA, CISA, FBI, Department of Energy, and EPA released a joint Cybersecurity Advisory (CSA) warning critical infrastructure owners and operators of an active cyber threat targeting Siemens S7 Series PLCs. The advisory describes an ongoing campaign in which threat actors conduct reconnaissance and capability development against U.S.-based Siemens PLC installations using AI-generated exploitation scripts disguised as legitimate monitoring tools. The authoring agencies emphasize this is not a theoretical risk but an active threat, and note that PLC targeting activity extends beyond Siemens devices to PLCs generally.

Water and Wastewater is named among the U.S. critical infrastructure sectors most targeted by this activity, alongside Critical Manufacturing, Energy, Chemical, Food and Agriculture, and Commercial Facilities.

Observed Techniques

The actors leverage internet scanning services (such as Censys and ZoomEye) to find internet-exposed PLCs running outdated software or that are otherwise poorly protected, take advantage of default or minimally configured credentials, and deploy AI-generated Python scripts. The agencies assess this pattern is likely persistent reconnaissance intended to develop capabilities and pre-position for future operational effects

against critical infrastructure. The advisory highlights that these risks are especially acute for asset owners who work with third-party service providers or system integrators with remote access, who may not realize their systems are exposed.

Affected Models:

- S7-200 Series (all CPU variants)
- S7-300 Series (all CPU variants, including 314, 315, 317 models)
- S7-400 Series (all CPU variants)
- S7-1200 Series (CPU 1211C, 1212C, 1214C, 1215C, 1217C variants)
- S7-1500 Series (all CPU variants, including F-series safety controllers)

WaterISAC strongly encourages members to review the full advisory and implement the authoring agencies' recommended defense-in-depth hardening steps. Entities that rely on systems integrators or third-party managed service providers are advised to share the advisory with those parties and request implementation of these mitigations.

Additional Reading

- Primary Mitigations to Reduce Cyber Threats to Operational Technology
- Siemens ProductCERT and Siemens CERT

Related WaterISAC PIRs: 6, 7, 7.1, 8, 10, 10.2, 12

Related Resources

MEMBERS ONLY

(TLP:AMBER+STRICT) Recent IOCs Shared in the WaterISAC Slack Workspace (August 20, 2026)

Aug 20, 2026 in Cybersecurity, Federal & State Resources, Security Preparedness

Tip of the Week – August 20, 2026

Aug 20, 2026 in Cybersecurity, Security Preparedness

MEMBERS ONLY

(TLP:GREEN) Joint MS-ISAC and WaterISAC Webinar – America's Critical Water Infrastructure Under Pressure

Aug 20, 2026 in Cybersecurity, OT-ICS

Security, Security Preparedness