Defending Against an Active Threat to Siemens S7 Series PLCs

Executive summary

Note: *This advisory relates to an active threat to Siemens S7 Series programmable logic controllers (PLCs). However, ongoing PLC targeting activity is broader than Siemens PLCs. All PLC owners and operators should apply relevant mitigations to reduce the risk to their devices and systems. The Siemens-specific content in this advisory should be understood and applied as one subset of the wider threat landscape.*

The National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), Department of Energy (DOE), and Environmental Protection Agency (EPA)—hereafter referred to as the authoring agencies—are releasing this Cybersecurity Advisory to warn owners and operators of industrial control systems (ICSs) of an active cyber threat to Siemens S7 Series PLCs and provide relevant mitigations to protect and defend them.

Top Mitigations

- **Inventory** all Siemens S7 Series programmable logic controllers (PLCs)
- **Apply** critical security patches
- **Ensure** PLCs are **not** accessible from the Internet
- **Strengthen** access controls
- **Monitor** for unauthorized activity
- **Harden** PLC services, protocols, and ladder logic integrity
- **Hunt** for anomalies that may indicate a compromise

The threat actors are conducting reconnaissance and capability development against U.S.-based Siemens PLC installations using AI-generated exploitation scripts disguised as legitimate monitoring tools. The actors leverage Internet scanning services to find Internet-exposed PLCs running outdated software or that are otherwise poorly protected. The U.S. critical infrastructure sectors most targeted by this threat activity include Critical Manufacturing, Energy, Water and Wastewater, Chemical, Food and Agriculture, and Commercial Facilities. This is not a theoretical risk—it is an active threat. Depending on the specific circumstances, exploitation of poorly protected PLCs

This document is marked TLP:CLEAR. Recipients may share this information without restriction. Information is subject to standard copyright rules.

could lead to disruption of critical industrial processes, safety incidents, downtime or equipment damage, compromise of sensitive data, compliance violations, and cascading impacts across interconnected systems.

The authoring agencies urge all owners and operators of operational technology (OT) systems using Siemens S7 Series and other PLC devices to proactively check their systems:

- are properly protected with all applicable security patches and updates,
- are isolated from the Internet wherever possible,
- have strong access controls, and
- employ security tooling to monitor ICS environments for anomalous or malicious activity.

These mitigations are particularly important for owners and operators who work with third-party service providers or system integrators who may have remote access to PLCs, as the asset owners may not realize that their systems are exposed and at risk.

Technical details

Note: This advisory uses the MITRE ATT&CK®[1] Matrix for ICS framework, version 19, and the MITRE ATT&CK Matrix for Enterprise framework, version 19. This advisory also uses MITRE D3FEND™, version 1.5.0. See **Appendix A** and **Appendix B** for tables of the activity mapped to MITRE ATT&CK and MITRE D3FEND tactics, techniques, and countermeasures.

Threat actor targeting

Threat actors are actively targeting the following Siemens PLC 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)

Threat actors are using AI assistance to generate exploitation scripts using publicly available information on these Siemens S7 Series PLCs for initial access, credential

[1] MITRE and ATT&CK are registered trademarks of The MITRE Corporation. MITRE D3FEND is a trademark of the MITRE Corporation.

access, denial of service, and other objectives. If these PLCs are exposed to the Internet or insufficiently segmented, then threat actors can exploit various critical and high severity known vulnerabilities in these PLCs.

Note: Using AI to generate exploitation scripts represents an evolution in threat actor capabilities, dramatically reducing the technical expertise and time required to develop working ICS exploitation scripts and malicious tools. In addition, AI enables adversaries to rapidly leverage additional attack vectors and adapt to defensive measures. Threat actors can easily collect public information about vulnerabilities and weaknesses, find exposed and exploitable PLCs, and use AI-generated scripts to act on that information. If PLCs are exposed to the Internet, they are at high risk for exploitation.

Threat actors are leveraging open source industrial automation libraries—specifically `snap7.dll`/`python-snap7`—combined with AI-assisted scripting to create custom tools that mimic legitimate OT monitoring solutions. These tools provide read/write access to Siemens S7 Series PLC memory, configuration data, and ladder logic programs via the S7comm protocol.

Threat actor techniques

Threat actors are:

- **Using Internet scanning services** (e.g., Censys, ZoomEye) to identify Internet-exposed or insufficiently segmented Siemens S7 Series PLCs [T1596.005]
- **Rapidly iterating exploit code** through AI-assisted development, lowering technical barriers to ICS attacks [T1587.004, T1588.007]
- **Taking advantage of insecure credentials** to access exposed devices that have unconfigured (default) or minimally configured authentication [T1694]
- **Deploying AI-generated Python scripts** that incorporate the `snap7.dll` library from public repositories [T0834] to gain read/write access to the PLC and mimic legitimate tools
- **Masquerading malicious scripts as legitimate monitoring tools** to evade detection by security teams [T0849]
- **Conducting read/write operations** on data blocks, potentially for reconnaissance, capability testing, or pre-positioning for effects operations [T0893, T0821]

The authoring agencies assess this activity pattern is likely intended as persistent reconnaissance in targeted sectors and facilities to develop capabilities and prepare to cause operational effects against critical infrastructure. For capability development, actors are testing and refining their exploitation techniques against specific PLC models to improve their ability to compromise the PLCs. To prepare for operational effects, actors are leveraging read access to understand target environments, enabling preparation and positioning for future write operations to cause disruption or other operational impacts.

Potential operational impacts

The U.S. critical infrastructure sectors most targeted by this threat activity include Critical Manufacturing, Energy, Water and Wastewater, Chemical, Food and Agriculture, and Commercial Facilities. Additionally, Siemens S7 Series PLCs are used in other sectors, including the Defense Industrial Base (DIB), and could be targeted there as well. Unauthorized access to PLCs could result in:

- **Disruption of critical industrial processes** affecting production throughput, product quality, and public services
- **Safety incidents affecting personnel** through manipulation of safety interlocks, emergency shutdown systems, or process parameters
- **Equipment damage and extended operational downtime** from process upsets, improper sequencing, or forced equipment operation outside design parameters
- **Compromise of sensitive operational data**, including proprietary process recipes, control strategies, and facility configurations
- **Cascading impacts across interconnected systems** affecting supply chains, dependent facilities, and integrated business operations
- **Regulatory compliance violations** and potential liability from process safety management failures

Mitigation actions

Since threat actors are developing capabilities using AI to compromise PLCs using known vulnerabilities, misconfigurations, and other weaknesses and then may use compromised PLCs to interfere with normal operations, the authoring agencies urge

organizations to implement comprehensive defense-in-depth strategies, in addition to Common Vulnerabilities and Exposures (CVE) remediation, to protect and defend their PLCs.

Detection opportunities

Organizations should implement detection strategies and hunt for anomalies that may indicate a compromise, focusing on [D3-PM]:

- **Anomalous S7comm behavior:** Connections from non-engineering workstations, unusual data block access patterns, or write operations outside change windows
- **Reconnaissance indicators:** Sequential IP scanning on port `102`, repeated connection attempts with varying parameters, or enumeration of CPU properties
- **Tool artifacts:** `Snap7.dll` library usage outside approved engineering workstations, Python scripts with S7comm functionality, or unauthorized monitoring software installations
- **Temporal anomalies:** S7comm activity during off-hours, unexpected connection patterns consistent with automated scripting rather than human operators, or configuration changes without corresponding work orders or change tickets
- **Geographic anomalies:** Connections originating from unexpected countries or IP ranges not associated with vendors or integrators

Preventative hardening actions

To counter threats to PLCs, the authoring agencies recommend all PLC owners and operators follow the mitigations in joint guidance Primary Mitigations to Reduce Cyber Threats to Operational Technology.

To harden Siemens S7 Series PLCs, the authoring agencies strongly urge all owners implement the hardening steps below. Entities that rely on systems integrators or third-party managed service providers should share this advisory with those parties and request implementation of the following mitigations:

1. Conduct an immediate inventory of all Siemens S7 Series PLCs in your environment [D3-HCI]:

- Verify current firmware versions for all S7-200, S7-300, S7-400, S7-1200, and S7-1500 controllers against backup gold copy
- Identify any systems directly or indirectly accessible from untrusted networks
- Map all engineering workstations with Totally Integrated Automation (TIA) Portal, STEP 7, or S7 programming access

2. Apply critical security patches as soon as possible [D3-SU]:

- Update Siemens S7 Series PLC firmware to the latest versions that address known vulnerabilities
- Prioritize Internet-facing or demilitarized zone (DMZ)-resident controllers
- Update TIA Portal and STEP 7 software to current versions
- Consult Siemens ProductCERT advisories for information on known vulnerabilities, along with relevant workarounds and mitigations
- Test all updates in a development environment before production deployment

3. Verify network segmentation and ensure PLCs are NOT accessible from the Internet [D3-NI]:

- Audit firewall rules for any exposed S7comm services (Transmission Control Protocol [TCP] port `102`)
- Block TCP port `102` at perimeter firewalls entirely
- Implement a DMZ architecture that separates OT and IT networks
- Deploy unidirectional gateways for data historian connections where appropriate
- Verify there is no unauthorized routing between corporate and industrial networks

4. Review and strengthen access controls [D3-NAM, D3-CH]:

- Restrict TIA Portal/STEP 7 access to authorized engineering workstations only by MAC/IP allowlisting on PLCs
- Enable PLC password protection on all Siemens S7 Series controllers
- Configure protection levels (such as write protection and read/write protection) on Siemens S7 Series devices

- Remove or change default SNMP community strings
- Implement application allowlisting on all engineering workstations
- Enable multi-factor authentication for all remote access to OT networks

5. Enable comprehensive logging and monitoring [D3-PM, D3-NTA]:

- Deploy ICS-aware intrusion detection (e.g., Claroty, Dragos Platform, Nozomi Networks, or similar)
- Monitor all S7comm traffic on TCP port `102` for connections outside maintenance windows
- Alert on unauthorized PUT/GET operations, especially write commands to data blocks or configuration areas of memory
- Log all TIA Portal/STEP 7 connections to PLCs with timestamps and source IPs
- Establish a baseline for legitimate behavior and configure monitoring tools to alert on deviations
- Monitor for Python processes with `snap7.dll` library imports on engineering workstations
- Watch for sequential IP scanning patterns or block reads of configuration data

6. Implement S7-specific hardening measures [D3-ACH]:

- Disable web servers on Siemens S7 Series devices if not operationally required
- Disable unused communication protocols (such as Modbus TCP and PROFINET, if they are not required)
- Configure connection resources to limit simultaneous S7comm sessions
- Enable TIA Portal/STEP 7 “complete restart protection” and “know-how protection” features where available
- Evaluate for ladder logic changes in online/offline modes

7. Contact Siemens for model-specific guidance:

- Engage Siemens Technical Support for hardening recommendations specific to your CPU models and firmware versions
- Verify patch compatibility with your specific operational environment and third-party integrations

- Request assistance with protection level configuration and access control implementation

Conclusion

There is an active threat targeting Internet-exposed Siemens S7 Series PLCs. The combination of known vulnerabilities, accessible exploitation libraries, and AI-assisted development creates a high-probability attack scenario against inadequately protected PLC installations. Organizations should treat this Cybersecurity Advisory with urgency and coordinate response efforts across security, engineering, executive leadership, plant operations, and vendor support teams to implement the recommended detection and hardening actions.

Resources

- Primary Mitigations to Reduce Cyber Threats to Operational Technology
- Secure connectivity principles for Operational Technology (OT): How organisations should design, secure, and manage connectivity in OT
- Control System Defense: Know the Opponent

Incident reporting

U.S. organizations are encouraged to report suspicious or criminal activity related to information in this advisory to CISA and/or the FBI. Contact CISA via CISA's 24/7 Operations Center at contact@cisa.dhs.gov or 1-844-Say-CISA (1-844-729-2472). File a claim with FBI's Internet Crime Complaint Center (IC3) or contact your local FBI field office. When available, please include the following information regarding the incident:

- Date, time, and location of the incident;
- Type of activity;
- Number of people affected;
- Type of equipment used for the activity; and
- Name of the submitting company or organization, and a designated point of contact.

Entities required to report incidents to DOE should follow established reporting requirements, as appropriate. For other energy sector inquiries, contact EnergySRMA@hq.doe.gov.

In addition, consider contacting Siemens ProductCERT via https://www.siemens.com/cert or email productcert@siemens.com.

Disclaimer of endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Purpose

This document was developed in furtherance of the authoring agencies' cybersecurity missions, including their responsibilities to identify and disseminate threats and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

Cybersecurity Report Feedback: CybersecurityReports@nsa.gov
Defense Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov
Media Inquiries / Press Desk: NSA Media Relations: 443-634-0721, MediaRelations@nsa.gov

Contact Siemens ProductCERT for up-to-date information about the security of Siemens products or to report cybersecurity vulnerabilities at productcert@siemens.com. For support with increasing the security of installed Siemens PLCs, contact Siemens Industrial Cybersecurity Services at services.automation@siemens.com. See Siemens ProductCERT and Siemens CERT for more information.

Appendix A: MITRE ATT&CK tactics and techniques

See **Table 2** for the threat actor tactics and techniques referenced in this advisory.

Table 1: MITRE ATT&CK tactics and techniques

Tactic	Technique Title	ID	Use
Reconnaissance	Search Open Technical Databases: Scan Databases	T1596.005	Using Internet scanning services to identify Internet-exposed or poorly segmented Siemens S7 Series PLCs
Resource Development	Develop Capabilities: Exploits	T1587.004	Developing exploits for known Siemens S7 Series PLC vulnerabilities
Resource Development	Obtain Capabilities: Artificial Intelligence	T1588.007	Rapidly iterating exploit code through AI-assisted development
Execution	Native API	T0834	Deploying AI-generated Python scripts incorporating the `snap7.dll` library
Execution	Modify Controller Tasking	T0821	Conducting write operations on data blocks, potentially for pre-positioning for effects operations
Evasion	Masquerading	T0849	Masquerading as legitimate monitoring tools to evade detection
Lateral Movement	Insecure Credentials	T1694	Accessing exposed devices that have unconfigured (default) or minimally configured authentication
Collection	Data from Local System	T0893	Conducting read operations on data blocks, potentially for reconnaissance

Appendix B: MITRE D3FEND countermeasures

See **Table 2** for a mapping of several of the cybersecurity countermeasures mentioned in this advisory.

Table 2: MITRE D3FEND Countermeasures

Countermeasure Title	ID	Description
Hardware Component Inventory	D3-HCI	Conduct an immediate inventory of all Siemens S7 Series PLCs
Software Update	D3-SU	Apply critical security patches as soon as possible
Network Isolation	D3-NI	Verify network segmentation and ensure PLCs are **not** accessible from the Internet
Network Access Mediation	D3-NAM	Restrict TIA Portal/STEP 7 access to authorized engineering workstations only via MAC/IP allowlisting on PLCs
Credential Hardening	D3-CH	• Enable PLC password protection on all S7 controllers • Enable multi-factor authentication for all remote access to OT networks
Platform Monitoring	D3-PM	• Deploy ICS-aware intrusion detection • Alert on unauthorized PUT/GET operations • Monitor for unexpected behavior deviations • Monitor for `snap7.dll` library imports • Hunt for indicators of compromise
Network Traffic Analysis	D3-NTA	• Alert on unexpected S7comm traffic on TCP port `102` • Watch for sequential IP scanning patterns
Application Configuration Hardening	D3-ACH	• Disable unused web servers and protocols • Remove SNMP community strings • Watch for ladder logic changes