censys ARC

ARC SITUATION REPORT · TLP:CLEAR

CISA Alert: Water Sector PLC Targeting

Rockwell/Allen-Bradley, Siemens, and Schneider Electric Exposure Assessment

REPORT ID	CISA-WWS-PLC-2026-07	**DATE**	July 30, 2026
SERIES	ICS/OT Threat Intelligence	**TLP**	TLP:CLEAR
SNAPSHOT	2026-07-30 (Censys Platform live index)	**SOURCE**	CISA Alert, July 30, 2026

CISA issued an alert on July 30, 2026 warning that threat actors are increasingly targeting internet-exposed programmable logic controllers (PLCs) in the Water and Wastewater Systems (WWS) sector, in some cases modifying passwords to lock out operators and disconnecting devices by changing their IP addresses, resulting in boil-water notices and sustained manual operations. CISA named Rockwell Automation/Allen-Bradley, Siemens, and Schneider Electric equipment and flagged cellular modems as a common blind spot in routine attack-surface scans. This report characterizes current Censys-observed internet exposure for each named vendor: **4,148** Rockwell/Allen-Bradley EtherNet/IP hosts, **4,117** Siemens SIMATIC S7-1200 hosts, and **2,072** Schneider Electric hosts (vendor-wide, not PLC-scoped), all as of the 2026-07-30 snapshot. This is an exposure characterization only: it does not confirm that any specific host is a victim of the activity CISA describes.

ADVISORY CONTEXT

The following paraphrases the CISA alert as supplied by the user for this report; it was not independently re-fetched from cisa.gov in this session.

CISA is observing a significant increase in threat actors targeting programmable logic controllers (PLCs) in the Water and Wastewater Systems (WWS) Sector. CISA urges critical infrastructure owners, operators, and integrators to remove publicly exposed PLCs and other operational technology (OT) from the internet as soon as possible. Observed actor behavior includes modifying PLC passwords to lock out operators and disconnecting PLCs by changing their IP addresses, producing boil-water notices and sustained manual operations at affected utilities.

Targeting affects water entities of all sizes, including organizations with mature cybersecurity processes. CISA specifically flags cellular modems installed by operators, vendors, or system integrators as a common blind spot: these connections may be undocumented and excluded from routine attack-surface scans. Owners of Rockwell Automation MicroLogix 1400 controllers are directed to Rockwell's guidance for restoring access when a controller password is unknown.

CISA-recommended mitigations

- Disconnect the PLC from the internet; route remote access through a VPN or gateway device, not directly to the PLC.
- Enable password protection and change default passwords.
- Allowlist IPs to permit remote access only from known engineering laptops or other critical OT assets.

This report addresses the exposure-characterization question only — current internet-facing host counts, geography, and network concentration for the three named vendors — and does not assess the mitigations above, IOC infrastructure, or attribution.

ROCKWELL/ALLEN-BRADLEY ETHERNET/IP

4,148 internet-exposed hosts respond to EtherNet/IP and self-identify as Rockwell Automation/Allen-Bradley. The United States remains dominant at 71.0% (2,945 hosts), with Canada a clear second at 11.5% (476 hosts).

Geographic Distribution

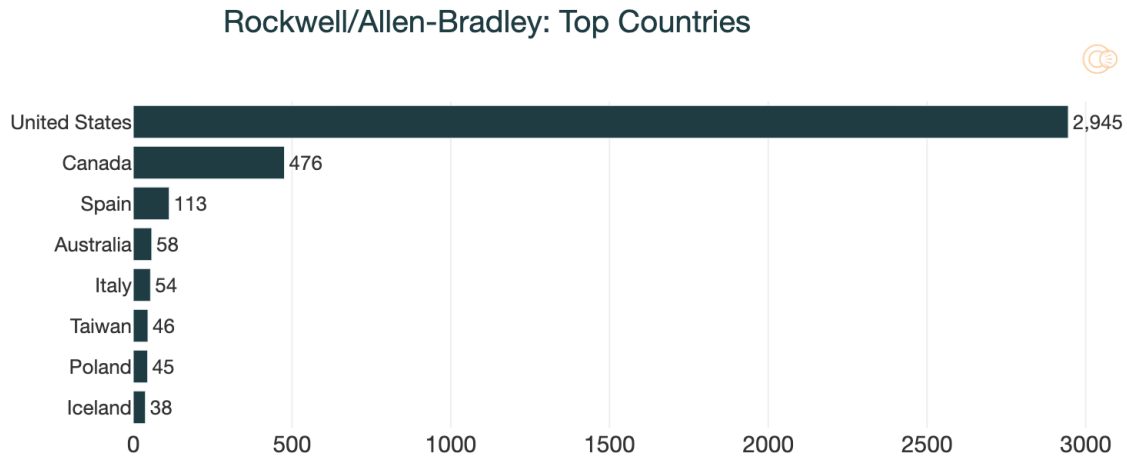

Figure: Rockwell/Allen-Bradley EtherNet/IP exposure by country (Censys, 2026-07-30).

Network / ASN Distribution

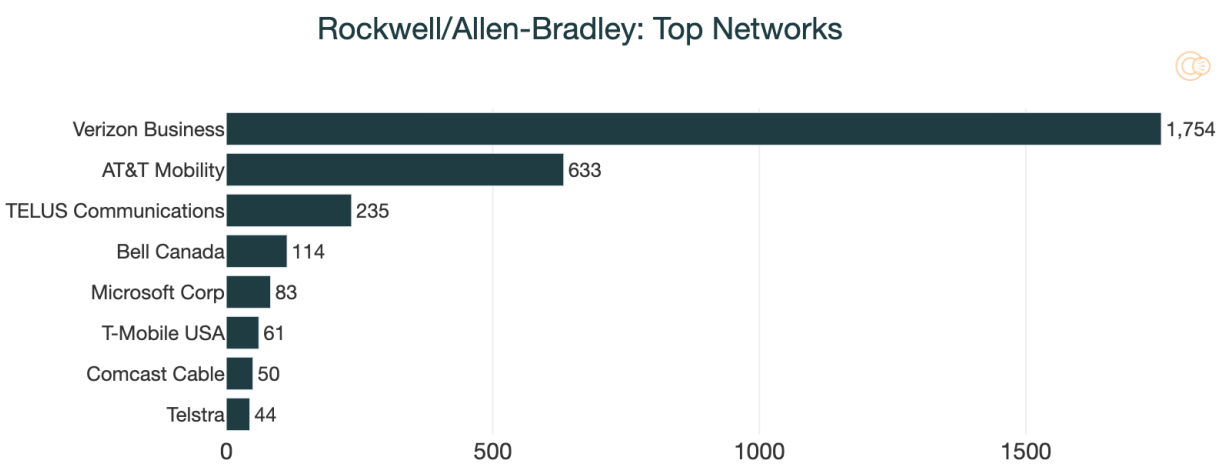

Figure: Rockwell/Allen-Bradley EtherNet/IP exposure by network/ASN (Censys, 2026-07-30).

Combined cellular carriers (Verizon Business, AT&T Mobility, T-Mobile USA) account for 59.0% of all exposed hosts.

SIEMENS SIMATIC S7-1200

4,117 internet-exposed hosts fingerprint as Siemens SIMATIC S7-1200. Exposure concentrates heavily in southern and central Europe: Greece, Spain, Italy, and Austria together account for 86.0% of the total, each dominated by that country's leading mobile carrier rather than fixed-line or hosting providers.

Geographic Distribution

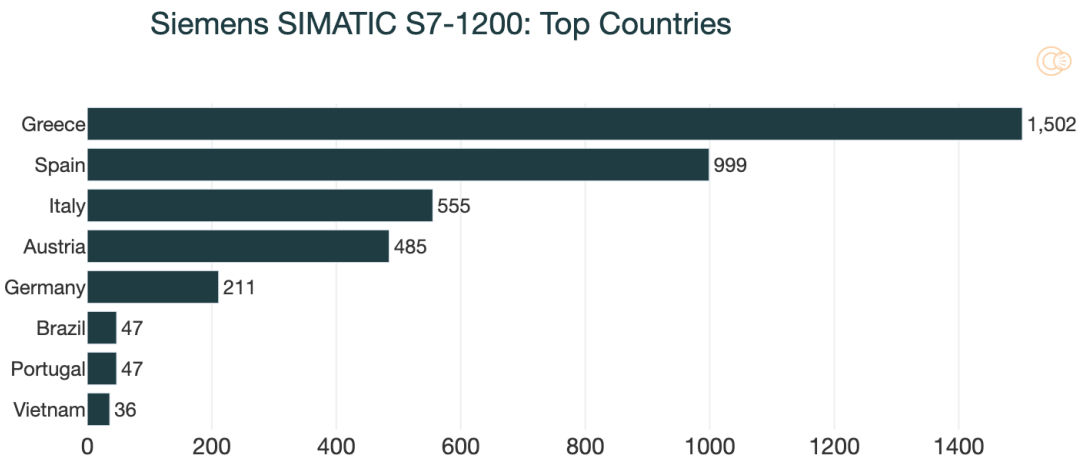

Figure: Siemens SIMATIC S7-1200 exposure by country (Censys, 2026-07-30).

Network / ASN Distribution

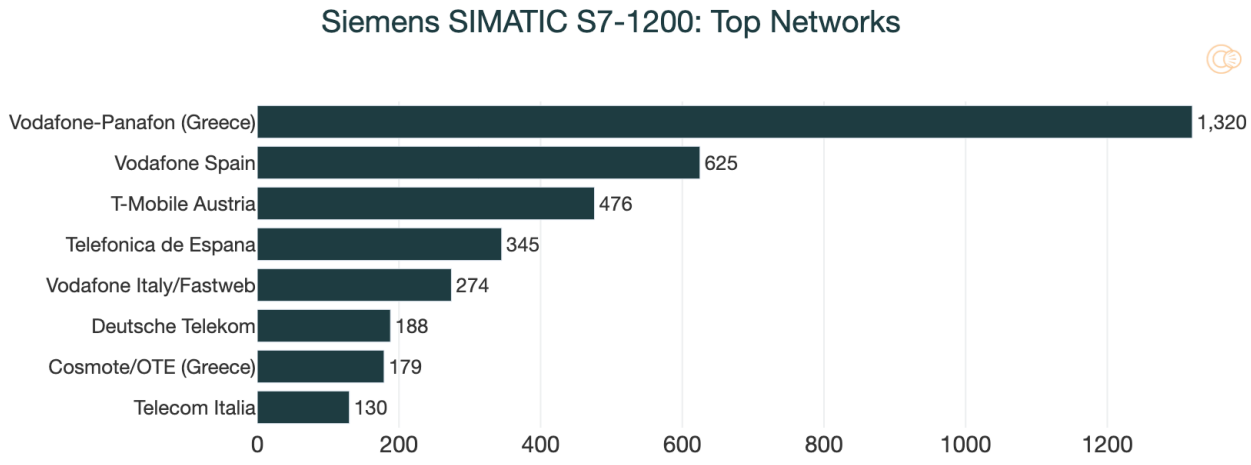

Figure: Siemens SIMATIC S7-1200 exposure by network/ASN (Censys, 2026-07-30).

SCHNEIDER ELECTRIC (VENDOR-WIDE)

2,072 internet-exposed hosts fingerprint as Schneider Electric hardware (snapshot 2026-07-30). **This query has no PLC-model or protocol filter.** This total should not be read as Schneider Electric PLC exposure specifically. Turkey and Australia account for 55.5% of the total combined.

Geographic Distribution

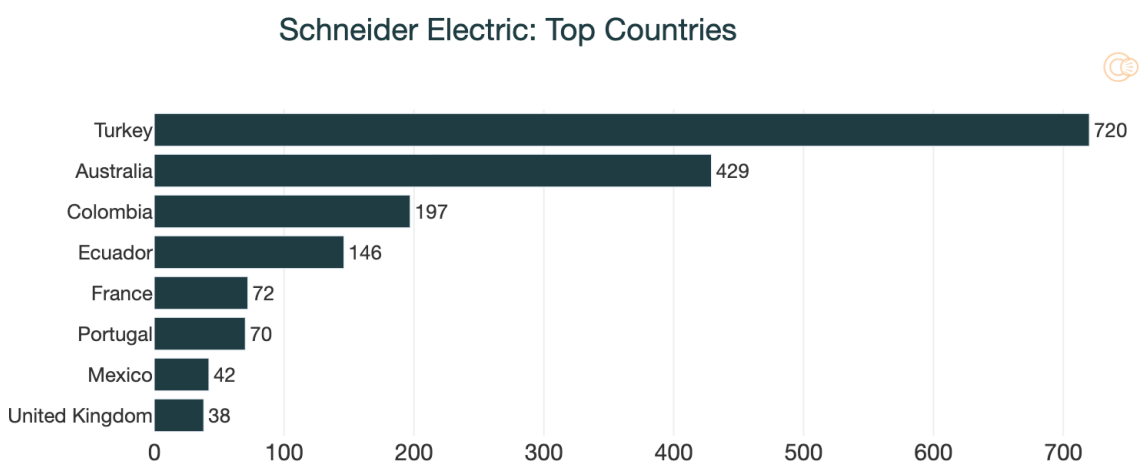

Figure: Schneider Electric (Vendor-Wide) exposure by country (Censys, 2026-07-30).

Network / ASN Distribution

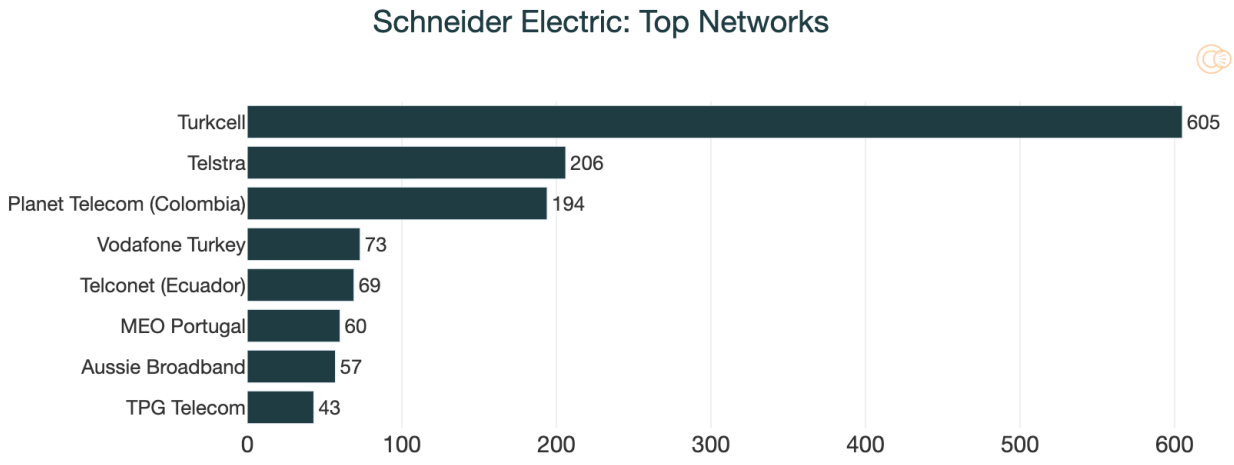

Figure: Schneider Electric (Vendor-Wide) exposure by network/ASN (Censys, 2026-07-30).

QUERIES

Rockwell/Allen-Bradley: `(host.services.protocol=EIP) and host.services.eip.identity.vendor_name="Rockwell Automation/Allen-Bradley"`

Siemens SIMATIC S7-1200: `host.hardware.vendor: "siemens" and host.hardware.product: "simatic_s7-1200"`

Schneider Electric: `host.hardware.vendor = "schneider-electric"`