ICS-CERT ADVISORY

ICSA-11-223-01A—A SUMMARY OF REPORTED ISSUES AFFECTING SIEMENS SIMATIC PLCS

UPDATE A

August 22, 2011

OVERVIEW

ICS-CERT has been coordinating multiple reports of issues affecting various models within the Siemens SIMATIC Step 7 (S7) programmable logic controller (PLC) product line. ICS-CERT has coordinated the issues with both Siemens and the researcher and continues to work with both entities.

A portion of the reported issues involve commands being transmitted using the International Organization for Standardization Transport Service Access Point (ISO-TSAP) protocol. According to ICS-CERT analysis, the ISO-TSAP protocol is functioning to specifications; however, authentication is not performed nor are payloads encrypted or obfuscated. Like ISO-TSAP, many protocols used in industrial control systems (ICSs) were designed with interoperability in mind and were intentionally designed without security features to be as open as possible. As a result, improving ICS security may require extensive architectural changes, including the addition of built-in or layered-on techniques to enhance protocol security. Changes necessary to improve protocol security could negatively impact interoperability and performance.

Some of the reported issues were coordinated and resolved with ICS-CERT and Siemens, while others were publicly released by the researcher without coordination. ICS-CERT's Vulnerability Disclosure Policy[a] encourages researchers to work directly with ICS-CERT and/or the affected vendor to disclose previously unknown vulnerabilities, so that patches and mitigations can be prepared and asset owners have adequate time to test and deploy them. Unless extenuating circumstances arise (e.g., active exploitation, threats of an especially serious nature, or danger to public health and safety), coordinated vulnerabilities are not publicly announced until patches/mitigations are available. The intent of this advisory is to provide a summary of the various alerts and notices as well as other public information available to date.

Some ICS-CERT products related to these reports are only available on the US-CERT Portal. Asset owners and operators can request access to the US-CERT Portal by sending an e-mail message to ICS-CERT@DHS.GOV.

a. ICS-CERT, *Vulnerability Disclosure Policy*, http://www.us-cert.gov/control_systems/ics-cert/disclosure.html, website last accessed August 11, 2011.

Table 1 outlines the public ICS-CERT Alerts that are currently available on the ICS-CERT website. Additional ICS-CERT products are available on the US-CERT Portal.

Table 1. ICS-CERT Siemens S7 Alert summary.

Date Published	Name	Description	Link
June 10, 2011	ICS-Alert-11-161-01, Siemens SIMATIC S7-1200 PLC Vulnerabilities	This public alert confirms the report of vulnerabilities affecting the S7-1200 and includes information on how to obtain the patch developed by Siemens.	Link
July 5, 2011	ICS-Alert -11-186-01, Password Protection Vulnerability in Siemens SIMATIC Controllers S7-200, S7-300, S7-400, S7-1200.	This public alert confirms that a portion of the vulnerabilities affecting the Siemens SIMATIC S7-1200 (ICS-Alert-11-161-01) also affect other models in the S7 product line.	Link
July 23, 2011	ICS-ALERT-11-204-01, S7-300 S7-400 Hardcoded Credentials	This public alert warns of an unanticipated, publicly disclosed vulnerability. An updated ALERT was subsequently released to clarify products affected (ICS-ALERT-11-204-01A) following ICS-CERT and Siemens analysis.	Link
July 29, 2011	ICS-ALERT-11-204-01A, (UPDATE A) S7-300 Hardcoded Credentials"	This alert updates ICS-ALERT-11-204-01 and contains the known affected products following ICS-CERT and Siemens analysis.	Link
August 3, 2011	ICS-ALERT-11-204-01B, (UPDATE B) S7-300 Hardcoded Credentials	This update alert warns of the public release of hardcoded credentials affecting certain Siemens S7-300 PLCs.	Link

Table 2 outlines public statements released by Siemens with regard to the issues affecting the SIMATIC S7 PLCs.

Table 2. Siemens statements on the SIMATIC S7 issues.

Date Published	Name	Description	URL
June 10, 2011	Version 1.0 - SIEMENS-SA-625789: Security Vulnerabilities in Siemens SIMATIC S7-1200 CPU	This Siemens Security Advisory discusses weaknesses in the SIMATIC S7-1200 CPU communication and authentication functions.	See updated version
June 10, 2011	SIMATIC Update: Information Regarding the Behavior of SIMATIC S7-1200 in Industrial Networks	This SIMATIC Update discusses certain weaknesses in the Ethernet network interface of the S7 1200	Link
July 5, 2011	Version 2.0 - SIEMENS-SA-625789: Security Vulnerabilities in Siemens SIMATIC S7-1200 CPU	This updated Siemens Security Advisory contains a modified CVSS score, solution, and version information.	Link
July 5, 2011	Potential Password Security Weakness in SIMATIC Controllers	This support article discusses a potential security weakness in the programming and configuration client software authentication mechanism employed by the SIMATIC S7 family of programmable controllers.	Link
July 29, 2011	SIMATIC Update: Security information about internal diagnostic functions in S7-300 PLCs	This update discusses the existence of an access method to internal diagnostic functions in the S7-300 PLCs.	Link

AFFECTED PRODUCTS

The reported issues affect various models in the Siemens SIMATIC S7 product line, including:

- S7-200
- S7-300
- S7-400
- S7-1200.

Please refer to ICS-CERT and Siemens statements provided in the Overview section Tables 1 and 2 and the Vulnerability Characterization section for information specific to each issue.

IMPACT

Multiple issues affecting the Siemens SIMATIC S7 PLC product line cause a variety of potential impacts. All reported issues require the attacker to have direct access to the PLC or access to the automation network to be successful. Access to the automation network allows an attacker complete control of the PLC, with the ability to execute unauthorized commands and read/write memory on the PLC. These unauthorized changes can result in the loss of process control, possibly causing damage to critical ICSs.

SIMATIC S7 PLCs can be installed in a myriad of applications ranging from food and beverage processing to energy utilities. Therefore, the exact impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of these vulnerabilities based on the environment, architecture, and product implementation.

BACKGROUND

Siemens SIMATIC S7 PLCs are used in a variety of industrial applications worldwide, including energy, water and wastewater, oil and gas, chemical, building automation, and manufacturing.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

This section categorizes all reported issues affecting the SIMATIC S7 product line that have been publicly disclosed. This section only includes reports that have been verified. Reported vulnerabilities that are unverified or still being coordinated with Siemens are not included here and are currently being handled in accordance with ICS-CERT's vulnerability policy.

Proof-of-concept modules have been developed to demonstrate many of the reported issues. These modules would lower the difficulty of exploitation. ICS-CERT is not aware that any of these modules are publicly available at this time.

ICS-CERT has categorized each of the reported issues into one of four general categories.

1. Use of an open communication protocol

This category relates to the use of an open protocol, ISO-TSAP, for communications. ISO-TSAP was not designed to be a secure protocol and is open to analysis. A PLC, its supporting engineering workstation software, and other tools are required to conduct this analysis. If the PLC is not configured with password

protection, any command that can be sent from the engineering workstation can be captured, modified, and replayed to the PLC.

2. Bypass of a password protection mechanism

This category relates to the ability to bypass a password mechanism that is in place to prevent unauthorized access to commands and actions on the PLC.

3. Denial-of-service (DoS) attacks putting the PLC into the stop/defective state

This category relates to DoS attacks that put the PLC into a defective state. The DoS issues do not exist because of the open protocol specification but are the result of the implementation or usage of the protocol.

4. Access to embedded software within the PLC and hardcoded credentials

This category relates to access to software that Siemens has embedded into the PLC, generally to support troubleshooting and diagnostics of the PLC.

The following tables address each of the publicly reported and verified vulnerabilities by category, affected models/versions, and the associated information product.

USE OF AN OPEN COMMUNICATION PROTOCOL

Table 3. Use of an open communication protocol.

Description	Models Affected	ICS-CERT Product
Read/Write of Memory	**Confirmed** • S7-1200 **Unconfirmed** • S7-200 • S7-300 • S7-400	Portal Alert Web Alert: ICS-ALERT-11-186-01
The ability to read and write PLC memory is allowed due to the design decision made to use ISO-TSAP, an inherently open protocol. Although this is commonly referred to as a vulnerability, ICS-CERT does not see this as a vulnerability in the protocol itself because the protocol was never designed to provide security or obfuscation. However, devices that implement this protocol have been shown to be vulnerable to exploitation.		

Description	Models Affected	ICS-CERT Product
Execution of commands over a clear-text, unauthenticated protocol	• S7-200 • S7-300 • S7-400 • S7-1200	Portal Alert Web Alert: ICS-ALERT-11-186-01
The ability to send commands to the PLC is allowed due to the design decision made to use ISO-TSAP, an inherently open protocol. Although this is commonly referred to as a vulnerability, ICS-CERT does not see this as a vulnerability in the protocol itself because the protocol was never designed to provide security or obfuscation. However, devices that implement this protocol have been shown to be vulnerable to exploitation.		

BYPASS OF A PASSWORD PROTECTION MECHANISM

Table 4. Bypass of a password protection mechanism.

Description	Models Affected	ICS-CERT Product
Bypass of a PLC password protection algorithm	• S7-200 • S7-300 • S7-400 • S7-1200 (Patched)	Portal Alert Web Alert: ICS-ALERT-11-186-01
If attackers can first capture the password sequence between the engineering workstation and the PLC, they can use that information to create a replay attack of password protected engineering workstation commands against PLCs using identical passwords.		
Unauthorized disabling of a password protection mechanism	**Confirmed:** • S7-1200 (Patched) **Unconfirmed:** • S7-200 • S7-300 • S7-400	Portal Alert
This vulnerability could be considered a subset of the “Bypass PLC Password Protection” vulnerability. If a stronger authentication mechanism were used, an attacker should not be able to disable this protection.		

DENIAL-OF-SERVICE VULNERABILITIES

Table 5. Denial-of-service (DoS) vulnerabilities.

Description	Models Affected	ICS-CERT Product
Denial-of-service (DoS) vulnerability in the Web server embedded in the PLC firmware	S7-1200 (Patched)	Portal Alert
An attacker can craft a DoS attack against the built-in web server on the S7-1200 PLC that forces it into a "stop/defective" state.		

ACCESS TO PLC EMBEDDED SOFTWARE AND HARDCODED CREDENTIALS

Table 6. Access to embedded software and hardcoded credentials.

Description	Models Affected	ICS-CERT Product
Authenticated diagnostic command shell through both TELNET and HTTP using hardcoded credentials	S7-300 (Not all versions are affected. See ICS-ALERT-11-204-01B.)	Web Alert: ICS-ALERT-11-204-01 ICS-ALERT-11-204-01A ICS-ALERT-11-204-01B
An attacker can use a hardcoded username and password to gain access to a diagnostic command shell. This shell gives the attacker the ability to perform various internal diagnostic functions and extract the contents of memory from the PLC.		

UNCONFIRMED POTENTIAL VULNERABILITIES

ICS-CERT is aware of reports of other potential vulnerabilities that are claimed to affect SIMATIC S7 PLCs. This information has not been coordinated directly with ICS-CERT or with Siemens. The available information relating to other potential vulnerabilities is being reviewed and evaluated by ICS-CERT and Siemens and, therefore, is not yet ready for public release.

MITIGATION

Both ICS-CERT and Siemens take these issues seriously and are working together to prepare a path forward for these and future issues. Currently, one patch is available that addresses two of the reported issues that affect S7-1200 PLCs.

--------- Begin Update A Part 1 of 1----------

Because of the design decisions made in the control system industry in the past to foster interoperability, it will not be possible to provide near-term patches for all of the reported issues.

--------- End Update A Part 1 of 1----------

In some cases, attempting to retrofit or patch these devices could break the communications required, potentially resulting in a loss of process control. For cases where patching is not possible, some near-term mitigations will be in the form of defense-in-depth practices until long-term architectural changes can be safely adopted, developed, and deployed.

Users of the Siemens SIMATIC S7 product line should consider employing all currently available mitigation strategies. These strategies include a patch developed by Siemens and other defensive measures to harden the automation network environment. ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

ICS-CERT continues to coordinate with Siemens to evaluate long-term mitigations, including patches, for remaining open issues.

SIEMENS PATCH FOR THE SIMATIC S7-1200

Siemens has released a patch that addresses two of the reported issues in the S7-1200 PLC. ICS-CERT has confirmed that the patch successfully resolves the bypass of a PLC password protection algorithm and DoS vulnerability, as reported by the researcher, in the web server that is embedded in the PLC firmware.

Where possible, ICS-CERT recommends that users of S7-1200 PLCs apply the patch developed by Siemens to help protect against potential exploitation of these vulnerabilities.

For more details about the vulnerabilities addressed by this patch, see "ICS-ALERT-11-161-01—Siemens SIMATIC S7-1200 PLC Vulnerabilities."[b]

Siemens' Security Advisory and patch are available at the following locations.

- Advisory: http://support.automation.siemens.com/WW/llisapi.dll/csfetch/50428932/Siemens_Security_Advisory_SSA-625789.pdf

b. ICS-ALERT-11-161-01, http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-161-01.pdf, website last accessed August 09, 2011.

- Patch: http://support.automation.siemens.com/WW/view/en/41886031/133100

DEFENSIVE MEASURES

Users of any of the Siemens SIMATIC S7 PLCs should consider employing defensive measures to improve the security posture of their automation network.

Configure and maintain user and administrative accounts using a strong account management policy.

- Enable password protection where possible.
- Use strong passwords.[c]
- Remove default accounts if unneeded. Change the password of default accounts that are needed.
- Disable all unused accounts.

Configure an intrusion detection system (IDS) to monitor traffic for unusual or unauthorized activity.

- Monitor traffic on the ISO-TSAP protocol, Port 102/TCP.
- Monitor traffic being unexpectedly sent outside the automation network.
- Monitor traffic between workstations. This traffic may be indicative of attacker pivoting through your network.

Use firewalls to manage communication to and within the automation network.

- Locate control system networks and remote devices behind firewalls and isolate them from the business network.
- Limit traffic on the automation network. Only allow necessary traffic from identified sources to communicate with the S7 PLCs.
- Allow only known and verified MAC addresses to communicate with appropriate resources on the automation network. For instance, do not permit a policy allowing any engineering workstation to communicate with all PLCs on the automation network.
- Block telnet and http traffic to PLCs even inside ICS network.
- Block SSL traffic into the automation network except what is required for proper operation. This action limits SSL tunneling.
- Manage workstations and other devices on the automation network.
- Enforce least-privilege user accounts. Do not grant permissions that are beyond what is needed to perform required actions.
- Use application whitelisting protection on engineering and operator workstations.
- Use virus protection on workstations. Ensure that the latest virus signature updates are deployed.

c. National Cyber Alert System Cyber Security Tip ST04-002, http://www.us-cert.gov/cas/tips/ST04-002.html, website last accessed August 09, 2011.

- Patch the Operating System and other software running on the workstation.
- If IDS or IPS devices are utilized on the control system network, consider adding a rule to watch for the string "Basisk."

Take measures to prevent social engineering attacks.

- Do not click web links or open unsolicited attachments in e-mail messages.
- Refer to *Recognizing and Avoiding Email Scams*[d] for more information on avoiding e-mail scams.
- Refer to *Avoiding Social Engineering and Phishing Attacks*[e] for more information on social engineering attacks.

In addition to the measures mentioned above, The Control Systems Security Program (CSSP) also provides a section for control systems security recommended practices on the CSSP web page. Several recommended practices are available for reading and download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.*[f]

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents. ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

d. US-CERT, *Recognizing and Avoiding Email Scams*, 2008, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed August 09, 2011.
e. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed August 09, 2011.
f. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed August 09, 2011.

ICS-CERT CONTACT

For any questions related to this report, please contact ICS-CERT at:

E-mail: ics-cert@dhs.gov
Toll Free: 1-877-776-7585
For CSSP Information and Incident Reporting: www.ics-cert.org

DOCUMENT FAQ

What is an ICS-CERT Advisory? An ICS-CERT Advisory is intended to provide awareness or solicit feedback from critical infrastructure owners and operators concerning ongoing cyber events or activity with the potential to impact critical infrastructure computing networks.