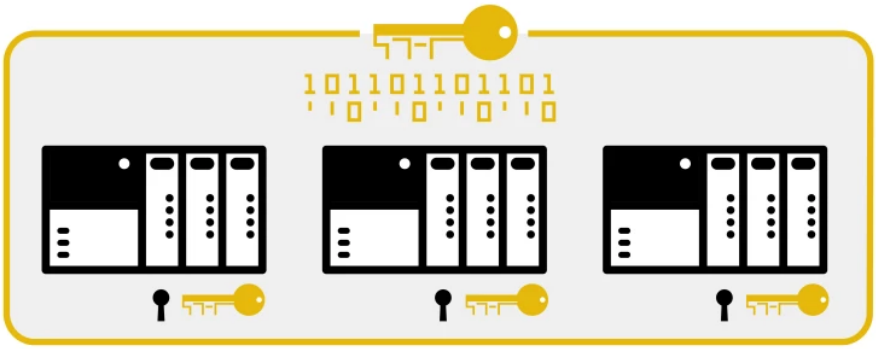
The Race to Native Code Execution in PLCs: Using RCE to Uncover Siemens SIMATIC S7-1200/1500 Hardcoded Cryptographic Keys

Team82 Research

October 11th, 2022



Executive Summary

- Team82 has developed a new, innovative method to extract heavily guarded, hardcoded, global private cryptographic keys embedded within the Siemens SIMATIC S7-1200/1500 PLC and TIA Portal product lines.
- An attacker can use these keys to perform multiple advanced attacks against Siemens SIMATIC devices and the related TIA Portal, while bypassing all four of its access level protections.
- A malicious actor could use this secret information to compromise the entire SIMATIC S7-1200/1500 product line in an irreparable way.
- All technical information was disclosed to Siemens, which released new versions of the affected PLCs and engineering workstation that address this vulnerability.
- CVE-2022-38465 has been assigned, and a CVSS v3 score of 9.3 was assessed.
- In addition, an attacker can develop an independent Siemens SIMATIC client (without requiring the TIA Portal) and perform full upload/download procedures, conduct man-in-the-middle attacks, and intercept and decrypt passive OMS+ network traffic.
- This work is an extension of our previous research into Siemens SIMATIC PLCs.
- Siemens has updated both the S7-1200 and S7-1500 PLCs and the TIA Portal, and urges users to move to current versions.
- This disclosure has led to the introduction of a new TLS management system in TIA Portal v17, ensuring that configuration data and communications between Siemens PLCs and engineering workstations is encrypted and confidential.

- Siemens' advisory can be found here. Siemens has also published a bulletin with remarks regarding its key protection update. Read it here.

Introduction

Close to 10 years ago, Siemens introduced asymmetric cryptography into the integrated security architecture of its TIA Portal v12 and SIMATIC S7-1200/1500 PLC CPU firmware families. This was done to ensure the integrity and confidentiality of devices and user programs, as well as for the protection of device communication within industrial environments.

Dynamic key management and distribution did not exist then for industrial control systems, largely because of the operational burden that key management systems would put on integrators and users. Siemens decided at the time instead to rely on fixed cryptographic keys to secure programming and communications between its PLCs and the TIA portal.

Since then, however, advances in technology, security research, and a swiftly changing threat landscape have rendered such hardcoded crypto keys an unacceptable risk. A malicious actor who is able to extract a global, hardcoded key, could compromise the entire device product line security in an irreparable way.

Team82 has to date conducted extensive research into PLC security, working closely with leading vendors to eradicate such practices as hardcoded keys, demonstrate the risk they pose to users' systems, and improve the overall security of the industrial automation ecosystem.

Our latest work—an extension of previous research conducted on Siemens SIMATIC S7-1200 and S7-1500 PLCs, as well as Rockwell Automation's Logix controllers and Studio 5000 Logix Designer—continues on that path.

We uncovered and disclosed to Siemens a new and innovative technique targeting SIMATIC S7-1200 and S7-1500 PLC CPUs that enabled our researchers to recover a global hardcoded cryptographic key (CVE-2022-38465) used by each Siemens affected product line. The key, if extracted by an attacker, would give them full control over every PLC per affected Siemens product line.

Using a vulnerability uncovered in previous research (CVE-2020-15782) on Siemens PLCs that enabled us to bypass native memory protections on the PLC and gain read and write privileges in order to remotely execute code, we were able to extract the internal, heavily guarded private key used across the Siemens product lines. This new knowledge allowed us to implement the full protocol stack, encrypt and decrypt protected communication, and configurations.

Siemens' response to this private disclosure led to an overhaul of the cryptographic schemes protecting its flagship PLC lines, as well as its TIA Portal engineering workstation application. Siemens acknowledged in a security advisory that existing protections around its hardcoded key are no longer sufficient, and invested the resources and time necessary to introduce a dynamic public-key infrastructure (PKI) that eliminates the use of hardcoded keys.

Siemens recommends users immediately update SIMATIC S7-1200 and S7-1500 PLCs and corresponding versions of the TIA Portal project to the latest versions. TIA Portal V17 and related CPU firmware versions include the new PKI system protecting confidential configuration data based on individual passwords per device and TLS-protected PG/PC and HMI communication, Siemens said in its advisory.

Technical Details

Siemens Access Restriction Mechanisms

A prominent security feature of Siemens PLCs is an access level restriction mechanism that is enforced with password protection. A password is configured within the project that is downloaded to the PLC along with a desired protection level. Those levels are:

- Level 1: Full read and write access to any configuration and logic block
- Level 2: Write protection:
    - Can read everything
    - Can change PLC modes
- Level 3: Limited read access:
    - Can read HMI data (values etc.)
    - Can read diagnostic data
- Level 4: Full protection
    - Cannot communicate with the PLC without password

ACCESS LEVELS	ACCESS RESTRICTION
Level 1 (no protection)	The hardware configuration and the blocks can be read and modified by anyone.
Level 2 (write protection)	With the access level, only read access is allowed without a password, which means that the following functions can be carried out: • reading the hardware configuration and the blocks • reading the diagnostic data • loading the hardware configuration and the blocks into the programming device. • changing the operating state (RUN/STOP) (not for S7-300 / S7-400 / WinAC) Without the password the following functions cannot be carried out: • loading the blocks and hardware configuration into the CPU • writing test functions • firmware update (online)
Level 3 (write/read protection)	At this access level, only • HMI acess and • reading diagnostic data is possible without a password. Without the password the following functions cannot be carried out: • loading the blocks and hardware configuration into or from the CPU, • writing test functions • changing the operating state (RUN/STOP) (not for S7-300 / S7-400 / WinAC) • Firmware update (online)
Level 4 (complete protection) S7-1200 (v4) S7-1500	With a complete protection, the CPU forbids: • read and write access to the hardware configuration and the blocks, • HMI access, • modifications in the server function for PUT/GET communication, • read and write access in the area “Accessible devices” and in the project for devices that are switched online.

Siemens S7 1200/1500 Access Levels (Source: Siemens)

All four levels use the same security mechanism to grant permissions to the user. The only difference between them is the extent of permissions granted with or without authentication. A password is requested upon any connection to the PLC.

Understanding S7-1200, S7-1500 Encryption

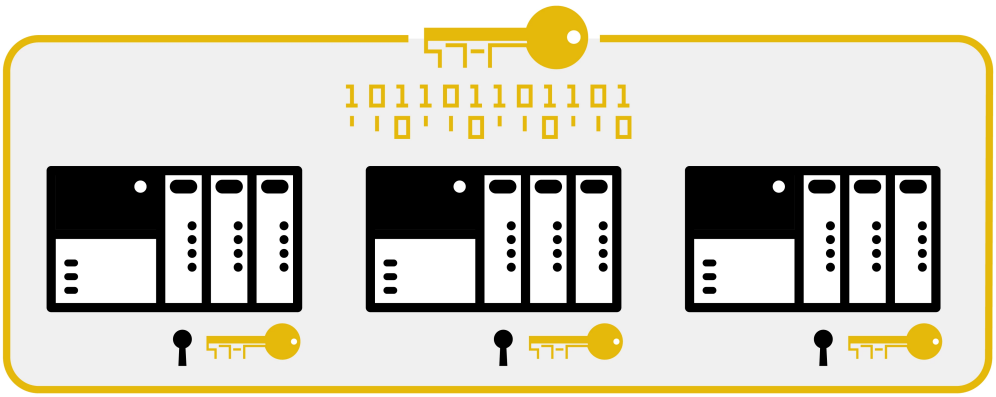
The asymmetric encryption procedures on the Siemens flagship PLCs has two principal purposes:

- Authentication: a shared derived session key that authenticates a user when communicating with a PLC.
- Confidentiality: encrypting data during portions of said communication, i.e., downloaded logic.

We were able to understand the encryption algorithm, which was based on Elliptic Curve asymmetric encryption. We found the curve parameters as well as an added complication: the use of a “configuration key” to further obfuscate and complicate the elliptical multiplication process.

Eventually we were able to uncover all the relevant keys involved in the encryption process:

- Connection Key: Used for packet integrity verification and authentication.
- CPU Key: A “per-model/firmware” (e.g S7-1518, S7-1517) key used to encrypt configurations, code, and maintain code integrity.
- Family Key: A “per-family” (e.g S7-1200, S7-1500) used for the same purposes as the CPU key, when the CPU key is not known.



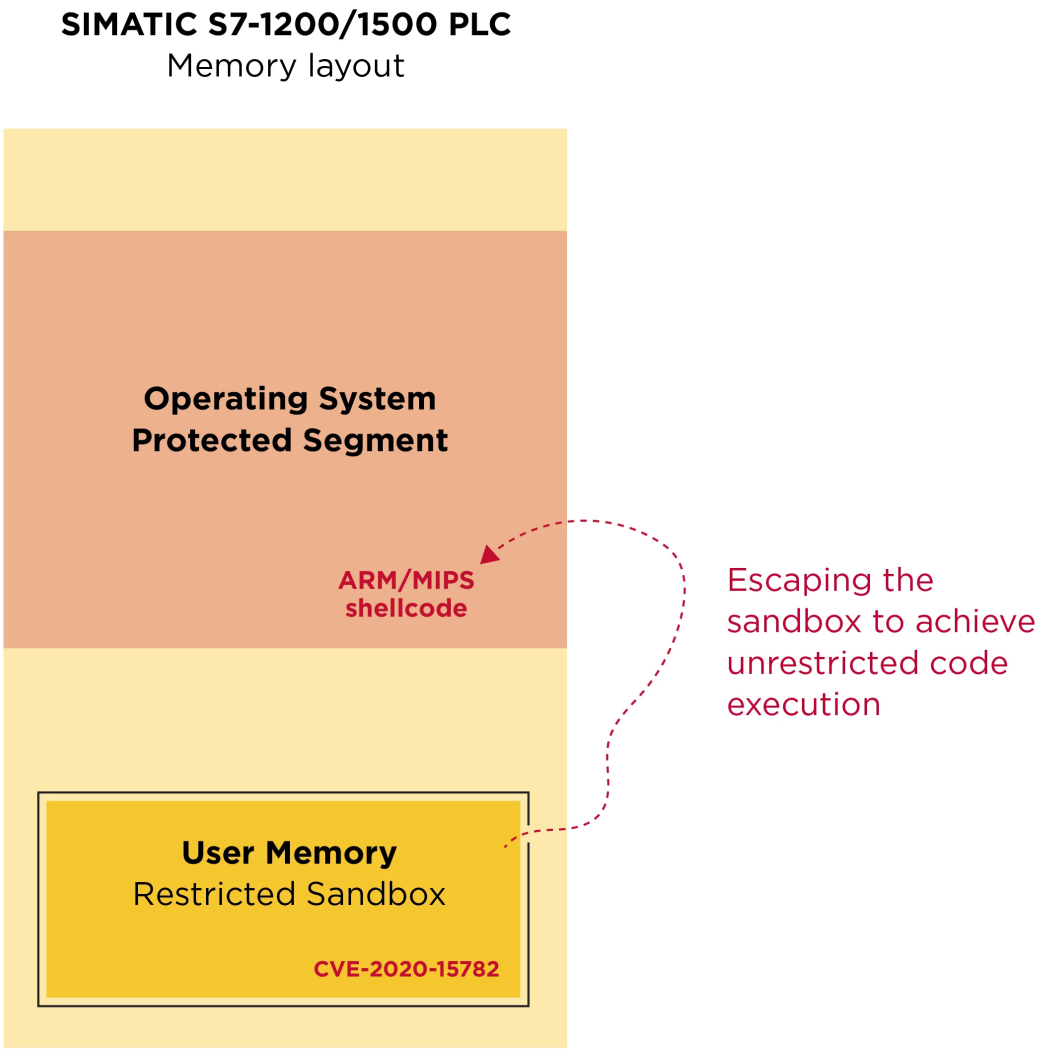
An illustration of the keys used in Siemens PLC encryption process.

Gaining Code Execution on the PLC

After reverse engineering one of Siemens SIMATIC .upd firmware S7-1200 which were unencrypted, we learned that the private key does not reside within the firmware files, therefore we would have to extract it somehow directly from the PLC.

In order to retrieve the private key from the PLC, we needed direct memory access (DA) to be able to search for it. To be able to perform DA actions, we searched and found a remote code execution vulnerability on both the 1200/1500

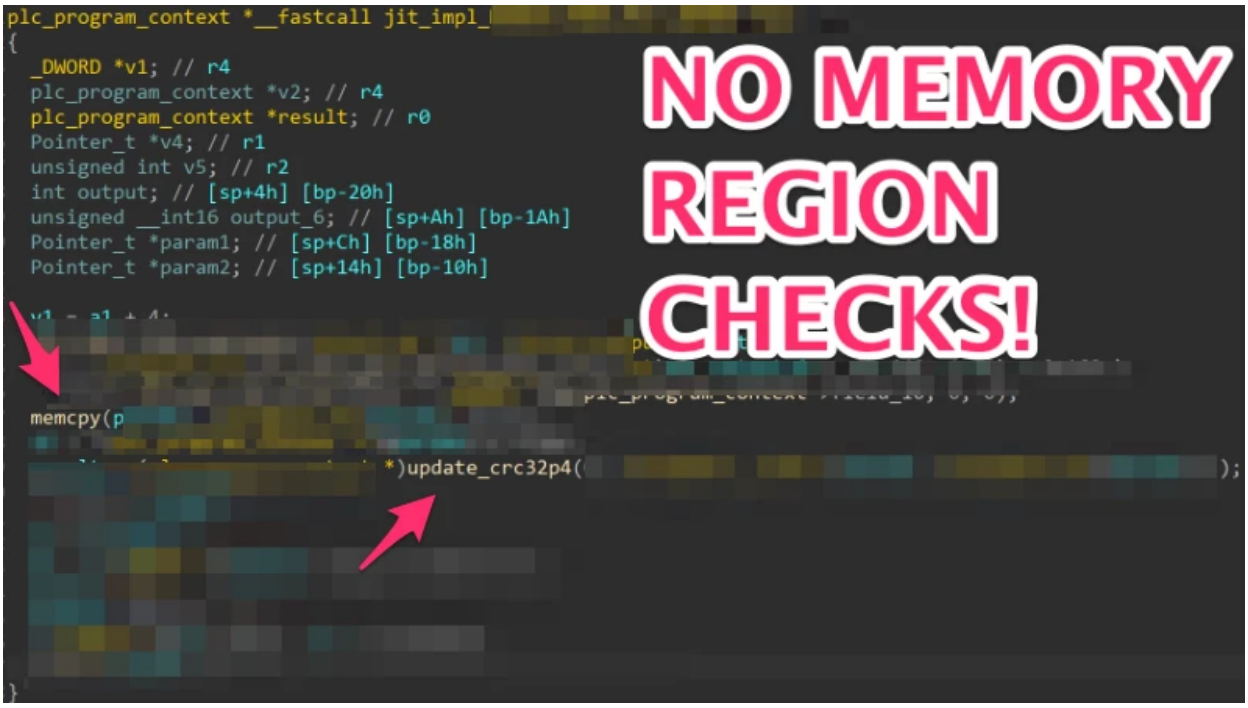
PLC series. The vulnerability (CVE-2020-15782) was triggered through a specific MC7+ function code containing our own crafted shellcode bytecode.



Our CVE-2020-15782 sandbox escape exploit.

The vulnerability logic for CVE-2020-15782 works as follows:

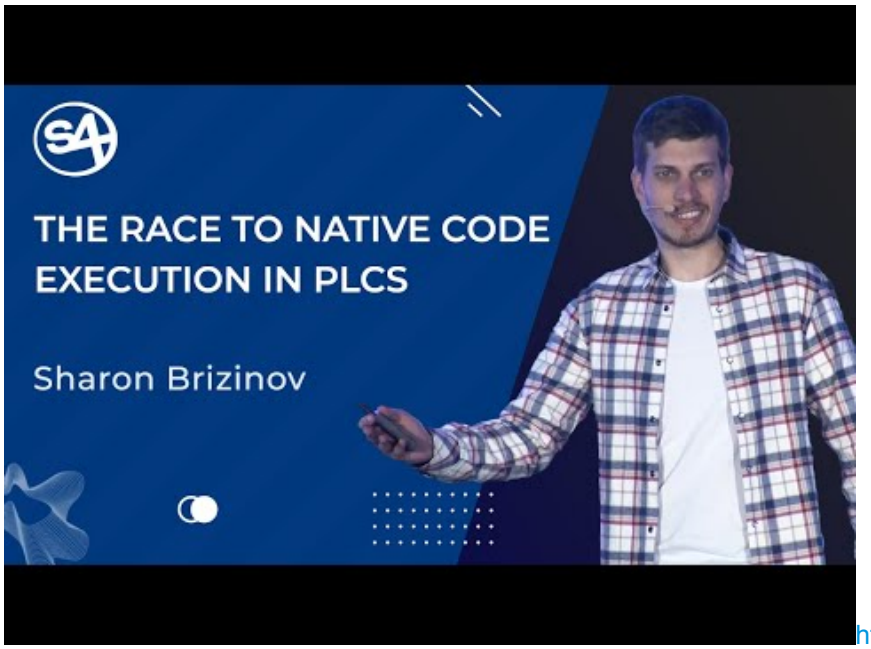
- Use [REDACTED] opcode, which has no security memory region checks, to copy an internal struct containing a native pointer to a valid memory area to a writable memory area
- Change the pointer inside this struct to our desired address
- Recalculate the CRC that was used to verify this struct (using the CRC32 opcode)
- Copy the struct back to its original location, now pointing to our desired address, using the [REDACTED] opcode
- At this point, we may use indirect access to the new address in our crafted struct.



MC7+ [REDACTED] opcode implementation function; since it missed the security memory memory region check it was possible to exploit it and achieve RCE (CVE-2020-15782).

We could now read or write from any memory address in the PLC. Using this capability, we could override native code and execute any desired native logic.

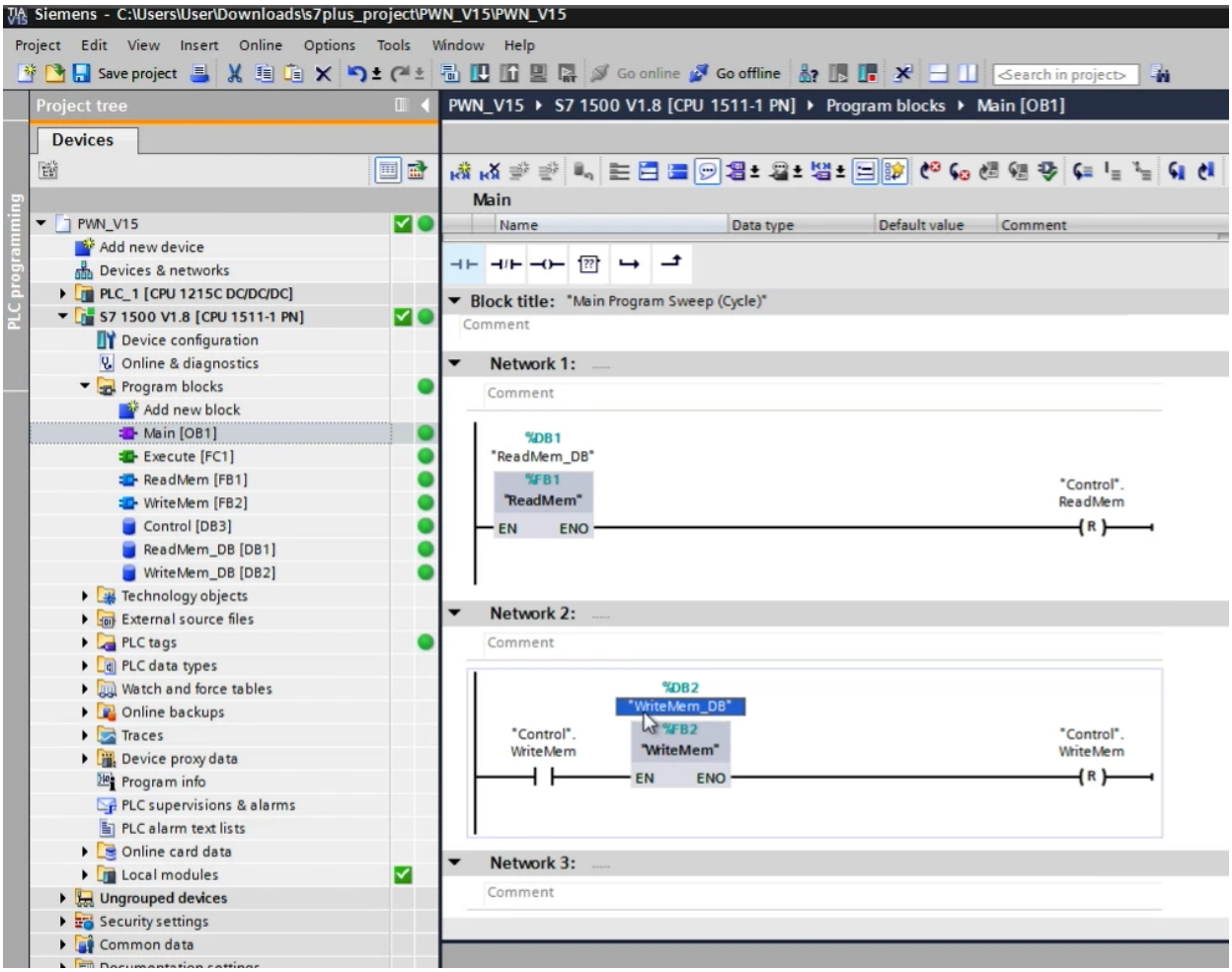
We gave a detailed technical presentation about this vulnerability at the S4x22 Conference, below:



https://youtu.be/r-dmxU1gEl0

Using the RCE to Obtain the Hidden Private Key

Using the DA read permission we obtained, we were able to extract the entire encrypted PLC firmware (SIMATIC S7-1500) and map its functions. During the mapping process we found a function that read the private key on the PLC.



The PoC we used to dump SIMATIC S7-1500 firmware from memory.

Once we had the function address, we rewrote the functionality of specific MC7+ opcodes with our shell code, forcing them to call the native function that reads the private key. We then copied the key to a known memory address and read it from there. Executing the overwritten function gave us the full private key of the PLC.

We later discovered that these keys are shared across each Siemens SIMATIC S7 product line, and immediately started a coordinated disclosure process with Siemens. This resulted in a new advisory and CVE-2022-38465.

Using the same methodology, we were able to extract the configuration key from the CPU.

Combining the private key, with the configuration key, and knowledge of the algorithm, allowed us to implement the full protocol stack, encrypt/decrypt protected communication, and configurations.

Demonstrating the vulnerability chain used to extract the private, global key.

Attack Flows: Gaining Control over a PLC and Process

Using the private key we were able to extract, an attacker may gain full control over a PLC.

Attacks on the Password

The attacks described below allow an attacker with knowledge of the PLC's private key and encryption algorithm, to retrieve the configured password on the PLC, thus gaining full control regardless of the protection level configured on the device.

- Obtain the Configuration and decrypt the password hash (reading configurations from the PLC): If the PLC is in a protection level lower than 3, An attacker can retrieve the configuration from the PLC (Upload procedure) with no special permission required. Once uploaded, the attacker has the PLC configuration and can use the private key to decrypt the password hash from the uploaded configuration. Using the decrypted password hash the attacker can authenticate to the PLC and gain higher privileges.
- Man in the Middle: An attacker with knowledge of the encryption mechanism of the traffic, as well as access to the private key, can impersonate the PLC in a connection. The man in the middle attack is performed in the following steps:
    - The client (victim) connects to the attacker's phony PLC and sends an encrypted connection key.
    - The attacker decrypts the connection key and uses the decrypted key to connect to the real PLC. Once connected, the attacker receives a password-based challenge.
    - The attacker forwards the real PLC's challenge to the client and receives a valid challenge response.
    - The attacker then forwards the challenge response to the real PLC to set up an authenticated connection. This session will be a fully privileged session. At this point, the attacker may change any configuration or blocks on the PLC, or read the configuration. This access includes the ability to read the encrypted password hash from the PLC and decrypt it.
- Passive Traffic Interception: An attacker with passive access to capture traffic to a given PLC on the network can intercept configuration reads/writes from the PLC. Using the private key, the attacker can decrypt the configuration and extract the password hash. With the password hash the attacker can authenticate to the controller and write a new configuration.

Summary

This attack (CVE-2022-38465) was made possible due to the ability to execute native code on S7 PLCs we achieved with our previous research CVE-2020-15782. Using native code execution, we were able to read the raw memory region protecting the private key and eventually fully recover the key.

By extracting the PLC's hardcoded private key, we were able to demonstrate multiple attack scenarios including decryption of all communication between S7 PLCs and an EWS, decryption of the configured password hash on the PLC, which we could use to gain full access to the PLC, conduct man-in-the-middle attacks, and more.

Users should update to current versions of the S7-1200 and S7-1500 PLC families, as well as TIA Portal v17, as advised by Siemens. TIA Portal v17 introduces a TLS management system in order to encrypt communication. Siemens also introduced a preactivated PLC configuration password requirement, that ensures all confidential PLC configuration data are protected by default as well as predefined secure PG/HMI communication, which prevents unsecured communication with other partners, and preactivated PLC access protection, that prevents any type of access to the controller unless explicitly configured.

The Vulnerability

CVE-2022-38465

CWE-522 Insufficiently Protected Credentials

CVSS v3 score: 9.3

Description: SIMATIC S7-1200, S7-1500 CPUs and related products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication.

Acknowledgment

Team82 would like to thank Siemens for its coordination in working through this disclosure, and for its swift response in confirming our findings and patching these vulnerabilities.