



Nro. Alerta:	EC-2022-092	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:	 <b>TLP:BLANCO</b>		
Fecha:	13-oct-2022	<b>USO DE RCE PARA DESCUBRIR CLAVES CRIPTOGRÁFICAS CODIFICADAS SIMATIC S7-1200/1500 DE SIEMENS</b>	V 1.1

## I. DATOS GENERALES:

**Clase de alerta:** Malware  
**Tipo de incidente:** Código malicioso  
**Nivel de riesgo:** Medio

## II. ALERTA.

RCE (Remote Control Execution), es uno de los tipos más peligrosos de vulnerabilidades informáticas. Permite a un atacante ejecutar código malicioso de forma remota dentro del sistema de destino en la red local o en Internet. No se requiere acceso físico al dispositivo.

Una vulnerabilidad RCE puede provocar la pérdida de control sobre el sistema o sus componentes individuales, así como el robo de datos confidenciales.

El equipo denominado "Team82", ha desarrollado un método nuevo e innovador para extraer claves criptográficas privadas globales fuertemente protegidas y codificadas integradas en las líneas de productos Siemens SIMATIC S7-1200/1500 PLC y TIA Portal.

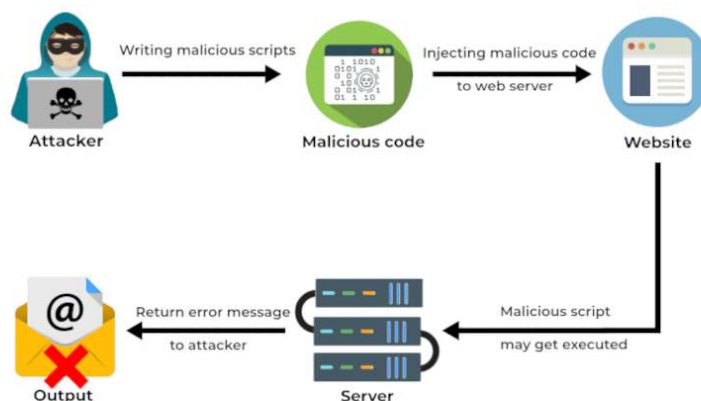




Figura 1.- Proceso lógico de un RCE Fuente: DRA

Nro. Alerta:	EC-2022-092	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	13-oct-2022	<b>USO DE RCE PARA DESCUBRIR CLAVES CRIPTOGRÁFICAS CODIFICADAS SIMATIC S7-1200/1500 DE SIEMENS</b>	V 1.1

### III. INTRODUCCIÓN.

Hace casi 10 años, Siemens introdujo la criptografía asimétrica en la arquitectura de seguridad integrada de sus familias de firmware de CPU de PLC TIA Portal v12 y SIMATIC S7-1200/1500. Esto se hizo para garantizar la integridad y confidencialidad de los dispositivos y programas de usuario, así como para proteger la comunicación de los dispositivos en entornos industriales.



La gestión y distribución de claves dinámicas no existían entonces para los sistemas de control industrial, en gran parte debido a la carga operativa que los sistemas de gestión de claves supondrían para los integradores y usuarios. Siemens decidió en ese momento confiar en claves criptográficas fijas para asegurar la programación y las comunicaciones entre sus PLC y el portal TIA.

Team82, ha realizado hasta la fecha una amplia investigación sobre la seguridad de los PLC, trabajando en estrecha colaboración con los principales proveedores para erradicar prácticas como las claves codificadas, demostrar el riesgo que representan para los sistemas de los usuarios y mejorar la seguridad general del ecosistema de automatización industrial.

Se ha descubierto una técnica nueva e innovadora dirigida a las CPU de PLC SIMATIC S7-1200 y S7-1500 que permitió a los investigadores recuperar una clave criptográfica codificada global (**CVE-2022-38465**) utilizada por cada línea de productos afectada de Siemens. La clave, si la extrae un atacante, le daría control total sobre cada PLC por línea de productos de Siemens afectada. El último trabajo, una extensión de la investigación anterior realizada en los PLC SIMATIC S7-1200 y S7-1500 de Siemens, así como en los controladores Logix de Rockwell Automation y Studio 5000 Logix Designer, continúa en ese camino.

Usando una vulnerabilidad descubierta en una investigación anterior (**CVE-2020-15782**) en los PLC de Siemens, permitió eludir las protecciones de memoria nativa en el PLC y obtener privilegios de lectura y escritura para ejecutar código de forma remota, se pudo extraer el código interno, en gran medida clave privada protegida utilizada en todas las líneas de productos de Siemens. Este nuevo conocimiento permitió implementar la pila de protocolos completa, cifrar y descifrar comunicaciones protegidas y configuraciones.



Nro. Alerta:	EC-2022-092	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:	 <b>TLP:BLANCO</b>		
Fecha:	13-oct-2022	<b>USO DE RCE PARA DESCUBRIR CLAVES CRIPTOGRÁFICAS CODIFICADAS SIMATIC S7-1200/1500 DE SIEMENS</b>	V 1.1

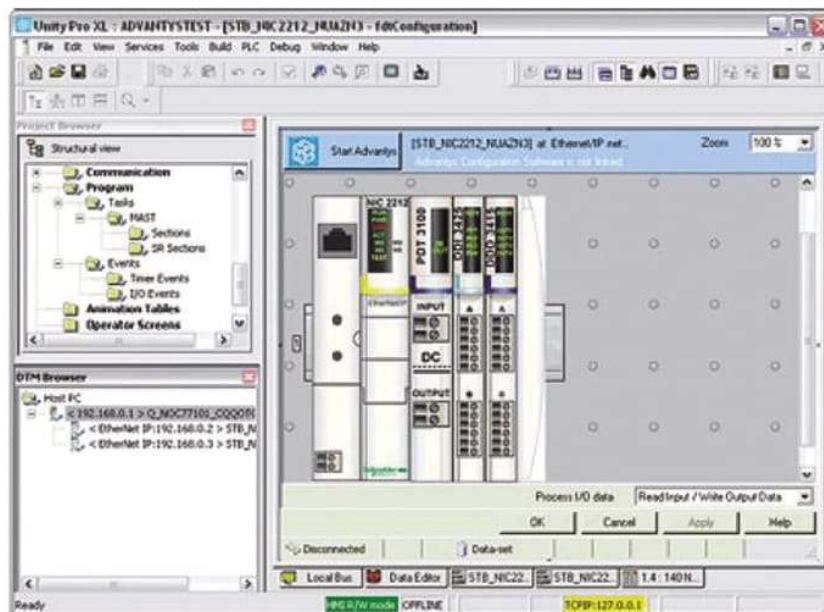


Figura 2.- Funcionamiento plataforma PLC, objetivo de RCE Fuente: DRA

Una característica de seguridad destacada de los PLC de Siemens es un mecanismo de restricción de nivel de acceso que se aplica con protección de contraseña. Se configura una contraseña dentro del proyecto que se descarga al PLC junto con un nivel de protección deseado. Esos niveles son:



#### Nivel 1:

Acceso completo de lectura y escritura a cualquier configuración y bloque lógico

#### Nivel 2:

Protección contra escritura:

- Puede leer todo
- Puede cambiar los modos de PLC

Nro. Alerta:	EC-2022-092	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	13-oct-2022	<b>USO DE RCE PARA DESCUBRIR CLAVES CRIPTOGRÁFICAS CODIFICADAS SIMATIC S7-1200/1500 DE SIEMENS</b>	V 1.1

### Nivel 3:

Acceso de lectura limitado:



- Puede leer datos HMI (valores, etc.)
- Puede leer datos de diagnóstico

### Nivel 4:

- Protección completa
- No se puede comunicar con el PLC sin contraseña.

ACCESS LEVELS	ACCESS RESTRICTION
<b>Level 1</b> (no protection)	The hardware configuration and the blocks can be read and modified by anyone.
<b>Level 2</b> (write protection)	With the access level, only read access is allowed without a password, which means that the following functions can be carried out: <ul style="list-style-type: none"> <li>• reading the hardware configuration and the blocks</li> <li>• reading the diagnostic data</li> <li>• loading the hardware configuration and the blocks into the programming device.</li> <li>• changing the operating state (RUN/STOP) (not for S7-300 / S7-400 / WinAC)</li> </ul> Without the password the following functions cannot be carried out: <ul style="list-style-type: none"> <li>• loading the blocks and hardware configuration into the CPU</li> <li>• writing test functions</li> <li>• firmware update (online)</li> </ul>
<b>Level 3</b> (write/read protection)	At this access level, only <ul style="list-style-type: none"> <li>• HMI access and</li> <li>• reading diagnostic data is possible without a password.</li> </ul> Without the password the following functions cannot be carried out: <ul style="list-style-type: none"> <li>• loading the blocks and hardware configuration into or from the CPU,</li> <li>• writing test functions</li> <li>• changing the operating state (RUN/STOP) (not for S7-300 / S7-400 / WinAC)</li> <li>• Firmware update (online)</li> </ul>
<b>Level 4</b> (complete protection) S7-1200 (v4) S7-1500	With a complete protection, the CPU forbids: <ul style="list-style-type: none"> <li>• read and write access to the hardware configuration and the blocks,</li> <li>• HMI access,</li> <li>• modifications in the server function for PUT/GET communication,</li> <li>• read and write access in the area "Accessible devices" and in the project for devices that are switched online.</li> </ul>

Figura 3.- Permisos de niveles de Acceso Siemens Fuente: DRA

Nro. Alerta:	EC-2022-092	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:	 <b>TLP:BLANCO</b>		
Fecha:	13-oct-2022	<b>USO DE RCE PARA DESCUBRIR CLAVES CRIPTOGRÁFICAS CODIFICADAS SIMATIC S7-1200/1500 DE SIEMENS</b>	V 1.1

Los cuatro niveles utilizan el mismo mecanismo de seguridad para otorgar permisos al usuario. La única diferencia entre ellos es el alcance de los permisos otorgados con o sin autenticación. Se solicita una contraseña en cualquier conexión al PLC. Los procedimientos de cifrado asimétrico en los PLC insignia de Siemens tienen dos propósitos principales:

- **Autenticación:** una clave de sesión derivada compartida que autentica a un usuario cuando se comunica con un PLC.
- **Confidencialidad:** cifrar datos durante partes de dicha comunicación, es decir, lógica descargada.

Después de realizar ingeniería inversa en uno de los firmware S7-1200 de SIMATIC .upd de Siemens que no estaban cifrados, se descubrió que la clave privada no reside en los archivos del firmware, por lo que se tendría que extraerla de alguna manera directamente del PLC.

Para recuperar la clave privada del PLC, se necesitaba acceso directo a memoria (DA) para poder buscarla. Para poder realizar acciones de DA, se procede con la búsqueda de una vulnerabilidad de ejecución remota de código en las series de PLC 1200/1500. La vulnerabilidad (CVE-2020-15782) se desencadenó a través de un código de función MC7+ específico que contenía el propio código de bytes de shellcode creado.



#### IV. VECTOR DE ATAQUE

Un atacante puede usar estas claves para realizar múltiples ataques avanzados contra los dispositivos SIMATIC de Siemens y el TIA Portal relacionado, al tiempo que elude las cuatro protecciones de nivel de acceso. Un actor malicioso podría usar esta información secreta para comprometer toda la línea de productos SIMATIC S7-1200/1500 de manera irreparable.

Toda la información técnica se reveló a Siemens, que lanzó nuevas versiones de los PLC afectados y la estación de trabajo de ingeniería que aborda esta vulnerabilidad. Se asignó CVE-2022-38465 y se evaluó una puntuación CVSS v3 de 9,3.

Además, un atacante puede desarrollar un cliente Siemens SIMATIC independiente (sin necesidad del TIA Portal) y realizar procedimientos completos de carga/descarga, realizar ataques de intermediario e interceptar y descifrar el tráfico de red OMS+ pasivo.



Nro. Alerta:	EC-2022-092	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	13-oct-2022	<b>USO DE RCE PARA DESCUBRIR CLAVES CRIPTOGRÁFICAS CODIFICADAS SIMATIC S7-1200/1500 DE SIEMENS</b>	V 1.1

Este trabajo es una extensión de nuestra investigación anterior sobre los PLC SIMATIC de Siemens.

Siemens ha actualizado los PLC S7-1200 y S7-1500 y el TIA Portal e insta a los usuarios a cambiar a las versiones actuales. Esta divulgación ha llevado a la introducción de un nuevo sistema de gestión TLS en TIA Portal v17, que garantiza que los datos de configuración y las comunicaciones entre los PLC de Siemens y las estaciones de trabajo de ingeniería estén encriptados y sean confidenciales.

La lógica de vulnerabilidad para **CVE-2020-15782** funciona de la siguiente manera:

- Use el código de operación [ELIMINADO], que no tiene controles de región de memoria de seguridad, para copiar una estructura interna que contiene un puntero nativo a un área de memoria válida a un área de memoria de escritura
- Cambie el puntero dentro de esta estructura a nuestra dirección deseada
- Vuelva a calcular el CRC que se usó para verificar esta estructura (usando el código de operación CRC32)
- Copie la estructura a su ubicación original, ahora apuntando a nuestra dirección deseada, usando el código de operación [ELIMINADO]



En este punto, podemos usar el acceso indirecto a la nueva dirección en nuestra estructura diseñada, ahora se podría leer o escribir desde cualquier dirección de memoria en el PLC. Usando esta capacidad, se puede anular el código nativo y ejecutar cualquier lógica nativa deseada.

## V. IMPACTO.

Usando el permiso de lectura DA obtenido, se puede extraer todo el firmware del PLC encriptado (SIMATIC S7-1500) y mapear sus funciones. Durante el proceso de mapeo se puede encontrar una función que lee la clave privada en el PLC.

Una vez que se obtiene la dirección de la función, se rescribe la funcionalidad de los códigos de operación MC7+ específicos con el código de shell, obligándolo a llamar a la función nativa que lee la clave privada. Luego se copia la clave a una dirección de memoria conocida y la leemos desde allí. La ejecución de la función sobrescrita nos dio la clave privada completa del PLC.



Nro. Alerta:	EC-2022-092	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	13-oct-2022	<b>USO DE RCE PARA DESCUBRIR CLAVES CRIPTOGRÁFICAS CODIFICADAS SIMATIC S7-1200/1500 DE SIEMENS</b>	V 1.1

Con esto, se descubrió que estas claves se comparten en todas las líneas de productos Siemens SIMATIC S7 e inmediatamente se inició un proceso de divulgación coordinado con Siemens. Esto resultó en un nuevo aviso y **CVE-2022-38465**.

Usando la misma metodología, pudimos extraer la clave de configuración de la CPU.

La combinación de la clave privada con la clave de configuración y el conocimiento del algoritmo permitió implementar la pila de protocolos completa, cifrar/descifrar la comunicación protegida y las configuraciones.





**Figura 3.- Metodología de extracción de clave Siemens** Fuente: DRA

Usando la clave privada extraída, un atacante puede obtener el control total de un PLC.

Los ataques que se describen a continuación permiten que un atacante con conocimiento de la clave privada y el algoritmo de encriptación del PLC, recupere la contraseña configurada en el PLC, obteniendo así el control total independientemente del nivel de protección configurado en el dispositivo.

- **Obtener la configuración y descifrar el hash de la contraseña** (lectura de configuraciones del PLC): si el PLC se encuentra en un nivel de protección inferior a 3, un atacante puede recuperar la configuración del PLC (procedimiento de carga) sin necesidad de un permiso especial. Una vez cargado, el atacante tiene la configuración del PLC y puede usar la clave privada para descifrar el hash de la contraseña de la configuración cargada. Usando el hash de contraseña descifrado, el atacante puede autenticarse en el PLC y obtener mayores privilegios.



Nro. Alerta:	EC-2022-092	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:	 <b>TLP:BLANCO</b>		
Fecha:	13-oct-2022	<b>USO DE RCE PARA DESCUBRIR CLAVES CRIPTOGRÁFICAS CODIFICADAS SIMATIC S7-1200/1500 DE SIEMENS</b>	V 1.1



- **Man in the Middle:** un atacante con conocimiento del mecanismo de encriptación del tráfico, así como acceso a la clave privada, puede hacerse pasar por el PLC en una conexión. El ataque del hombre en el medio se realiza en los siguientes pasos:
  - ✓ El cliente (víctima) se conecta al PLC falso del atacante y envía una clave de conexión cifrada.
  - ✓ El atacante descifra la clave de conexión y usa la clave descifrada para conectarse al PLC real. Una vez conectado, el atacante recibe un desafío basado en contraseña.
  - ✓ El atacante reenvía el desafío del PLC real al cliente y recibe una respuesta de desafío válida.
  - ✓ Luego, el atacante reenvía la respuesta de desafío al PLC real para establecer una conexión autenticada. Esta sesión será una sesión totalmente privilegiada. En este punto, el atacante puede cambiar cualquier configuración o bloque en el PLC, o leer la configuración. Este acceso incluye la capacidad de leer el hash de la contraseña cifrada del PLC y descifrarlo.
- **Intercepción de tráfico pasivo:** un atacante con acceso pasivo para capturar tráfico a un PLC determinado en la red puede interceptar lecturas/escrituras de configuración desde el PLC. Usando la clave privada, el atacante puede descifrar la configuración y extraer el hash de la contraseña. Con el hash de contraseña, el atacante puede autenticarse en el controlador y escribir una nueva configuración.

## VI.RECOMENDACIONES.

- La respuesta de Siemens a esta divulgación privada condujo a una revisión de los esquemas criptográficos que protegen sus líneas de PLC insignia, así como su aplicación de estación de trabajo de ingeniería TIA Portal. Siemens reconoció en un aviso de seguridad que las protecciones existentes en torno a su clave codificada ya no son suficientes e invirtió los recursos y el tiempo necesarios para introducir una infraestructura dinámica de clave pública (PKI) que elimina el uso de claves codificadas.
- Siemens recomienda a los usuarios actualizar inmediatamente los PLC SIMATIC S7-1200 y S7-1500 y las versiones correspondientes del proyecto TIA Portal a





Nro. Alerta:	EC-2022-092	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:	 <b>TLP:BLANCO</b>		
Fecha:	13-oct-2022	<b>USO DE RCE PARA DESCUBRIR CLAVES CRIPTOGRÁFICAS CODIFICADAS SIMATIC S7-1200/1500 DE SIEMENS</b>	V 1.1

las últimas versiones. TIA Portal V17 y las versiones de firmware de CPU relacionadas que incluyen el nuevo sistema PKI que protege los datos de configuración confidenciales basados en contraseñas individuales por dispositivo y comunicación PG/PC y HMI protegida por TLS.

## VII. DESCARGO DE RESPONSABILIDAD.

La información en la presente alerta; se proporciona solo con fines informativos. El EcuCERT de la ARCOTEL, no respalda ningún producto o servicio comercial, incluidos los sujetos de análisis.



Cualquier referencia a productos, procesos o servicios comerciales específicos por marca de servicio, marca comercial, fabricante o de otro modo, no constituye ni implica respaldo, recomendación o favorecimiento por parte del EcuCERT de la ARCOTEL.

La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

## VIII. REFERENCIAS.

- <https://claroty.com/team82/research/the-race-to-native-code-execution-in-plcs-using-rce-to-uncover-siemens-simatic-s7-1200-1500-hardcoded-cryptographic-keys>
- <https://www.emerson.com/en-us/automation/control-and-safety-systems/programmable-automation-control-systems?gclid=CjwKCAjw7p6aBhBiEiwA83fGugryW3eLEhzCtRdPJ5jAEgK064h8NyJrDG-XR IEV1PVwX4gV1VrwBoCkGoQAvD BwE>
- <https://www.protect.airbus.com/blog/remote-code-execution-on-ecostruxure-plc-simulator-cve-2020-28211-cve-2020-28212-cve-2020-28213/>
- <https://csirt.telconet.net/tag/rce/>
- <https://encyclopedia.kaspersky.com/glossary/remote-code-execution-rce/>
- <https://claroty.com/team82>



Nro. Alerta:	EC-2022-092	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR  <b>ALERTAS DE SEGURIDAD</b>	
TLP:	 <b>TLP:BLANCO</b>		
Fecha:	13-oct-2022	<b>USO DE RCE PARA DESCUBRIR CLAVES CRIPTOGRÁFICAS CODIFICADAS SIMATIC S7-1200/1500 DE SIEMENS</b>	V 1.1

