Vulnerabilidades ICS

Termómetro CCI - 2

26 de junio de 2020

Centro de Ciberseguridad Industrial

www.CCI-es.org

Tabla de contenido

Profesional de la Ciberseguridad industrial desde hace diez años en distintas empresas como Schneider Electric, S21sec, EY, SecurityMatters, Forescout y Telefónica y miembro activo del ecosistema del Centro de Ciberseguridad Industrial (CCI) desde 2013, profesional Nivel Negro y participando como autor y revisor de distintos estudios y documentos realizados por este.

Introducción

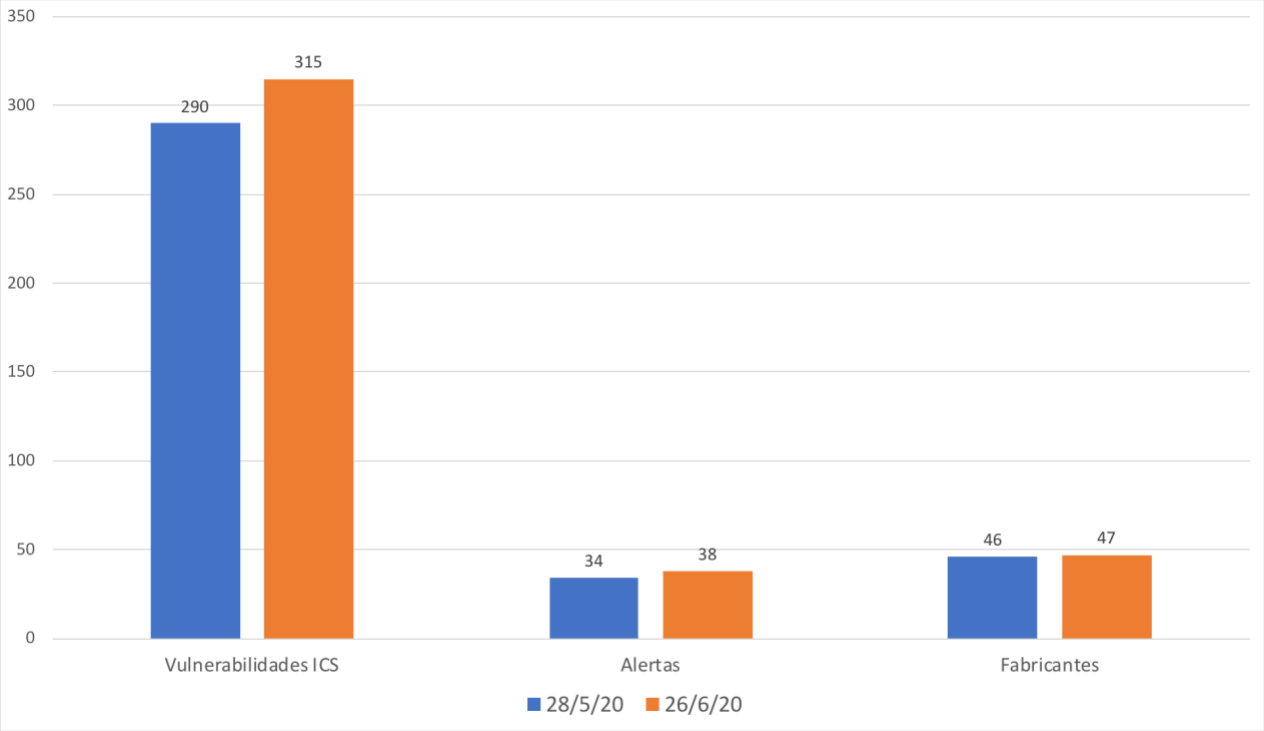
Desde la publicación del cuaderno “Una década de vulnerabilidades ICS” el 4 de mayo de 2020, se han seguido publicando nuevas vulnerabilidades sobre sistemas ICS, lo que ha hecho variar la exposición al riesgo de los fabricantes recogidos en dicho cuaderno.

Desde el CCI queremos mantener actualizada esta información para proporcionar una visión de la evolución de estas vulnerabilidades para que el ecosistema pueda utilizarlas cómo precise en una publicación que denominaremos **Termómetro de vulnerabilidades ICS del CCI**.

En cada actualización publicaremos:

- Evolución del número de fabricantes de control incluidos en el termómetro para el periodo en curso
- Evolución de vulnerabilidades y alertas de los fabricantes de control incluidos en el termómetro
- El mapa de calor de exposición al riesgo de los fabricantes, actualizado a fecha de publicación.
- Comentarios acerca de la evolución del mapa de riesgo.

Fabricantes y vulnerabilidades ICS



Nuevos fabricantes

En esta edición del termómetro CCI, se incluye un nuevo fabricante:

Riesgo Bajo	Riesgo Medio	Riesgo Alto	Riesgo Muy Alto
N/A	N/A	N/A	Swarco

Nuevas vulnerabilidades

El número de vulnerabilidades ICS publicadas por el NIST desde la última actualización es de **25.**

Nuevas alertas

El número de Alertas ICS publicadas por el **NIST** desde la última actualización es de **4.**

Schneider Electric Easergy T300

Swarco CPU LS4000

GE RT Clock RT430

Wago PFC 200

Mapa de riesgo

27 de junio de 2020

	Johnson Controls Meinberg Omron RuggedCom	Post Oak Swarco Yokogawa		
MICROSYS Mitsubishi Electric Panasonic Sierra Wireless Tesla	Beckhoff Emerson GE Phoenix Contact Rockwell Universal Robots	Advantech		Moxa
Fuji Electric Gemalto Honeywell Systech Triangle MicroWorks			Schneider Electric	ABB Siemens WAGO
3S-Smart Aveva Dahua Digi EasyIO Eaton eWON General Electric Hikvision Insulet LAquis SCADA Mikrotik Opto 22 OSIsoft Philips ProSoft Westermo				

Cambios en el riesgo de fabricante

Schneider Electric

Pasa de riesgo **Bajo** a riesgo **Alto**, al publicarse **13** nuevas vulnerabilidades con **1** alerta en el periodo.

CVE	Date published	CVSS	Warning	Description
CVE-2020-7505	2020-06-16	9.0	⚠	A CWE-494 Download of Code Without Integrity Check vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow an attacker to inject data with dangerous content into the firmware and execute arbitrary code on the system.
CVE-2020-7512	2020-06-16	7.5		A CWE-1103: Use of Platform-Dependent Third Party Components with vulnerabilities vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow an attacker to exploit the component.
CVE-2020-7497	2020-06-16	7.5		A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists in EcoStruxure Operator Terminal Expert 3.1 Service Pack 1 and prior (formerly known as Vijeo XD)which could cause arbitrary application execution when the computer starts.
CVE-2020-7503	2020-06-16	6.8		A CWE-352: Cross-Site Request Forgery (CSRF) vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow an attacker to execute malicious commands on behalf of a legitimate user when xsrf-token data is intercepted.
CVE-2020-7493	2020-06-16	6.8		A CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability exists in EcoStruxure Operator Terminal Expert 3.1 Service Pack 1 and prior (formerly known as Vijeo XD) which could cause malicious code execution when opening the project file.
CVE-2020-7494	2020-06-16	6.8		A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists in EcoStruxure Operator Terminal Expert 3.1 Service Pack 1 and prior (formerly known as Vijeo XD) which could cause malicious code execution when opening the project file.
CVE-2020-7509	2020-06-16	6.5		A CWE-269: Improper privilege management (write) vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow an attacker to elevate their privileges and delete files.
CVE-2020-7506	2020-06-16	5.0		A CWE-538: File and Directory Information Exposure vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow an attacker to pack or unpack the archive with the firmware for the controller and modules using the usual tar archiver resulting in an information exposure.
CVE-2020-7507	2020-06-16	5.0		A CWE-400: Uncontrolled Resource Consumption vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow an attacker to login multiple times resulting in a denial of service.

CVE	Date published	CVSS	Warning	Description
CVE-2020-7513	2020-06-16	5.0		A CWE-312: Cleartext Storage of Sensitive Information vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow an attacker to intercept traffic and read configuration data.
CVE-2020-7508	2020-06-16	5.0		A CWE-307 Improper Restriction of Excessive Authentication Attempts vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow an attacker to gain full access by brute force.
CVE-2020-7504	2020-06-16	5.0		A CWE-20: Improper Input Validation vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow an attacker to disable the webserver service on the device when specially crafted network packets are sent.
CVE-2020-7495	2020-06-16	4.3		A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability during zip file extraction exists in EcoStruxure Operator Terminal Expert 3.1 Service Pack 1 and prior (formerly known as Vijeo XD) which could cause unauthorized write access outside of expected path folder when opening the project file.

SWARCO

Entra directamente en la lista con riesgo **Muy Alto**, al publicarse **1** nueva vulnerabilidad con **1** alerta en el periodo:

CVE	Date published	CVSS	Warning	Description
CVE-2020-12493	2020-05-29	10.0	⚠	An open port used for debugging in SWARCOs CPU LS4000 Series with versions starting with G4... grants root access to the device without access control via network. A malicious user could use this vulnerability to get access to the device and disturb operations with connected devices.

GE

Continúa con riesgo Medio, aunque contabiliza **1** alerta en el periodo contemplado:

CVE	Date published	CVSS	Warning	Description
CVE-2020-12017	2020-06-02	9.0	⚠	GE Grid Solutions Reason RT Clocks, RT430, RT431, and RT434, all firmware versions prior to 08A05. The device's vulnerability in the web application could allow multiple unauthenticated attacks that could cause serious impact. The vulnerability may allow an unauthenticated attacker to execute arbitrary commands and send a request to a specific URL that could cause the device to become unresponsive. The unauthenticated attacker may change the password of the 'configuration' user account, allowing the attacker to modify the configuration of the device via the web interface using the new password. This vulnerability may also allow an unauthenticated attacker to bypass the authentication required to configure the device and reboot the system.

Wago

Continúa con riesgo **Alto,** aunque contabiliza **1** alerta en el periodo contemplado:

CVE	Date published	CVSS	Warning	Description
CVE-2020-6090	2020-06-11	9.0	⚠	An exploitable code execution vulnerability exists in the Web-Based Management (WBM) functionality of WAGO PFC 200 03.03.10(15). A specially crafted series of HTTP requests can cause code execution resulting in remote code execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.

Siemens

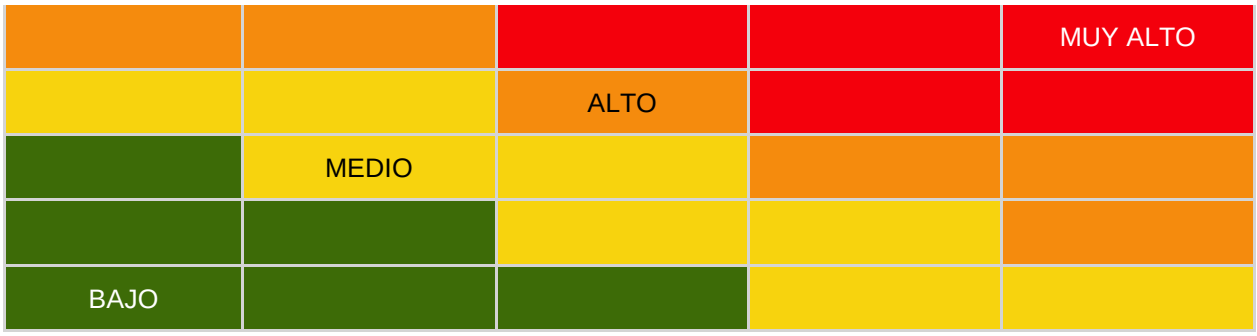
Continua en riesgo **Alto**, al publicarse **4** nuevas vulnerabilidades en el periodo:

CVE	Date published	CVSS	Warning	Description
CVE-2020-7580	2020-06-10	7.2		A vulnerability has been identified in SIMATIC Automation Tool (All versions), SIMATIC NET PC software (All versions V16 < V16 Upd3), SIMATIC PCS 7 (All versions), SIMATIC PCS neo (All versions), SIMATIC ProSave (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC STEP 7 (All versions < V5.6 SP2 HF3), SIMATIC STEP 7 (TIA Portal) V13 (All versions), SIMATIC STEP 7 (TIA Portal) V14 (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions), SIMATIC WinCC OA V3.16 (All versions < P018), SIMATIC WinCC OA V3.17 (All versions < P003), SIMATIC WinCC Runtime Advanced (All versions), SIMATIC WinCC Runtime Professional V13 (All versions), SIMATIC WinCC Runtime Professional V14 (All versions), SIMATIC WinCC Runtime Professional V15 (All versions), SIMATIC WinCC Runtime Professional V16 (All versions), SIMATIC WinCC V7.4 (All versions < V7.4 SP1 Update 14), SIMATIC WinCC V7.5 (All versions < V7.5 SP1 Update 3), SINAMICS STARTER commissioning tool (All versions), SINAMICS Startdrive (All versions), SINEC NMS (All versions), SINEMA Server (All versions), SINUMERIK ONE virtual (All versions), SINUMERIK Operate (All versions). A component within the affected application regularly calls a helper binary with SYSTEM privileges while the call path is not quoted.
CVE-2020-7589	2020-06-10	6.4		A vulnerability has been identified in LOGO!8 BM (incl. SIPLUS variants) (All versions). The vulnerability could lead to an attacker reading and modifying the device configuration and obtain project files from affected devices. The security vulnerability could be exploited by an unauthenticated attacker with network access to port 135/tcp. No user interaction is required to exploit this security vulnerability. The vulnerability impacts confidentiality, integrity, and availability of the device. At the time of advisory publication no public exploitation of this security vulnerability was known.
CVE-2020-7586	2020-06-10	4.6		A vulnerability has been identified in SIMATIC PCS 7 (All versions), SIMATIC PDM (All versions), SIMATIC STEP 7 V5.X (All versions < V5.6 SP2 HF3), SINAMICS STARTER (containing STEP 7 OEM version) (All versions < V5.4 HF1). A buffer overflow vulnerability could allow a local attacker to cause a Denial-of-Service situation. The security vulnerability could be exploited by an attacker with local access to the affected systems. Successful exploitation requires user privileges but no user interaction. The vulnerability could allow an attacker to compromise the availability of the system as well as to have access to confidential information.
CVE-2020-7585	2020-06-10	4.6		A vulnerability has been identified in SIMATIC PCS 7 (All versions), SIMATIC PDM (All versions), SIMATIC STEP 7 V5.X (All versions < V5.6 SP2 HF3), SINAMICS STARTER (containing STEP 7 OEM version) (All versions < V5.4 HF1). A DLL Hijacking vulnerability could allow a local attacker to execute code with elevated privileges. The security vulnerability could be exploited by an attacker with local access to the affected systems. Successful exploitation requires user privileges but no user interaction. The vulnerability could allow an attacker to compromise the availability of the system as well as to have access to confidential information.

ANEXO – I: Cálculo del mapa de riesgo

Con objeto de mostrar de una manera gráfica y rápida la postura de cada fabricante en lo que se refiere al riesgo asociado a las vulnerabilidades publicadas, he seleccionado un formato gráfico muy común en la gestión de Riesgos: el mapa de calor.

Este diagrama presenta distintos colores para representar el riesgo asociado de manera cualitativa y en cuatro rangos: Bajo, Medio, Alto y Muy Alto.



La posición de cada fabricante dentro del mapa depende de los valores obtenidos en dos parámetros asociados con la **probabilidad** (Número de CVEs publicados) y el **impacto** de dichos CVEs (Valor medio de CVSS).

Para cada año, se ha calculado cada uno de estos valores entre 1 y 5.

- En el eje horizontal, se ha calculado el valor proporcional al número de CVEs publicados para ese fabricante en un año concreto en comparación con el fabricante con mayor número de CVEs.

- En el eje vertical se ha calculado el valor medio de CVSS de los CVEs publicados ese año y se ha dividido entre 2.

Para intentar dar una idea más cualitativa en lo que se refiere a la postura de cada fabricante, se han introducido dos correcciones en el cálculo:

- Si el fabricante tiene algún CVE ese año considerado cómo Alerta (Acceso por la red, complejidad baja e impacto completo en disponibilidad), se incrementa en una unidad el impacto (Eje vertical) y en una unidad la probabilidad (Eje horizontal). Esto se realiza para diferenciar a este fabricante de otros sin este tipo de CVEs y posicionarlo en una zona de mayor riesgo.

- De la misma manera, si un fabricante tiene algún CVE ese año con un valor CVSS de 10.0, se incrementa en una unidad la probabilidad (Eje horizontal). Esto se realiza para diferenciar a este fabricante de otros sin este tipo de CVEs y posicionarlo en una zona de mayor riesgo.

Se ha estudiado mediante distintas simulaciones que estas correcciones no suponen grandes alteraciones en la postura global del riesgo de ese fabricante y, sin embargo, presentan un diagnóstico cualitativo más ajustado.

Centro de Ciberseguridad Industrial

www.cci-es.org