



Centro de
Ciberseguridad Industrial

Vulnerabilidades ICS Termómetro CCI 2021- 12

📍 PASEO DE LAS DELICIAS, 30 - 2º

28045 MADRID

☎ +34 910 910 751

✉ INFO@CCI-ES.ORG

🌐 WWW.CCI-ES.ORG

B BLOG.CCI-ES.ORG

🐦 [@INFO_CCI](https://twitter.com/INFO_CCI)



Tabla de contenido

<i>Introducción</i>	5
<i>Novedades 2021</i>	5
<i>Fabricantes y debilidades ICS</i>	6
<i>Nuevos fabricantes</i>	6
<i>Nuevas debilidades</i>	7
<i>Nuevas alertas</i>	8
<i>Mapa de riesgo</i>	10
<i>Cambios en el riesgo de fabricante</i>	11
<i>ANEXO – I: Cálculo del mapa de riesgo</i>	12
<i>ANEXO II – Vulnerabilidades publicadas por elNIST desde el último termómetro CCI</i>	13



Profesional de la Ciberseguridad industrial desde hace más de diez años en distintas empresas como Schneider Electric, S21sec, EY, SecurityMatters, Forescout, Telefónica y actualmente en TITANIUM Industrial Security.

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 como precise en una publicación que denominaremos **Termómetro de vulnerabilidades ICS del CCI**.

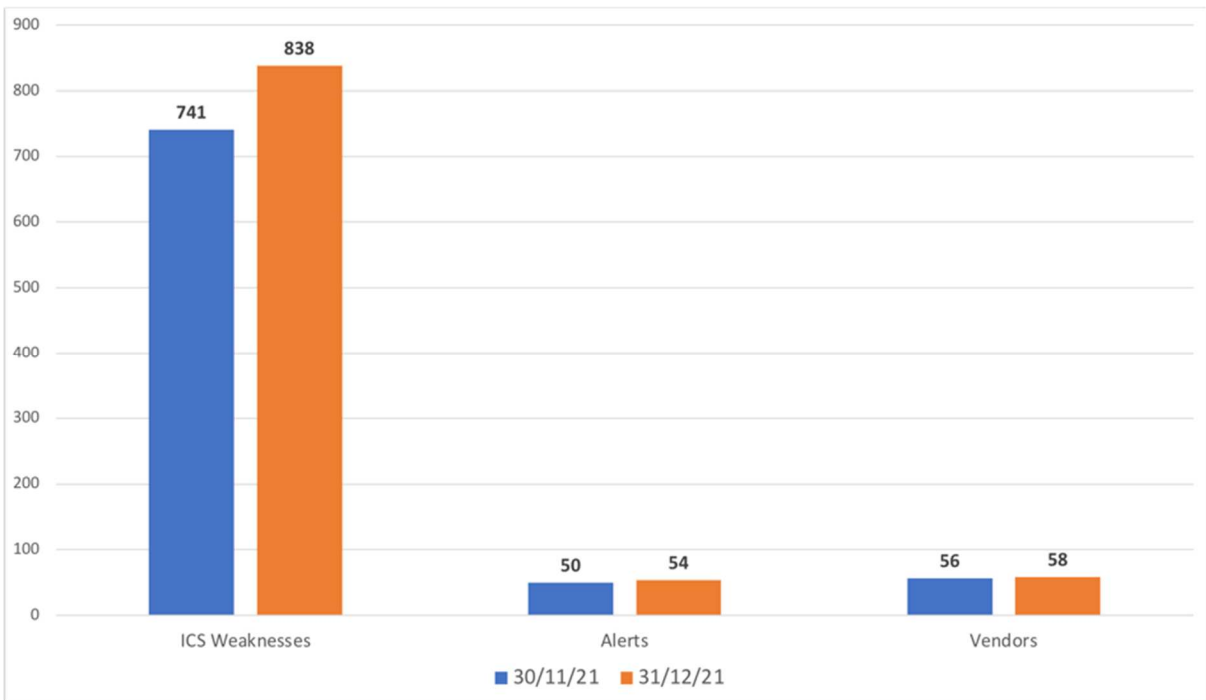
En cada actualización publicaremos:

- Evolución del número de fabricantes de sistemas 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.

Novedades 2021

Para adaptarnos a la creciente casuística de vulnerabilidades públicas que afectan a varios fabricantes, en el año 2021 se aplicará un nuevo criterio, publicando cada uno de los fabricantes afectados por esta única vulnerabilidad (CVE). Para ser coherentes con este nuevo acercamiento, en 2021 hablaremos de “Debilidades ICS” (ICS Weaknesses) para dar cabida a estas vulnerabilidades multifabricante.

Fabricantes y debilidades ICS



Nuevos fabricantes

En esta edición del termómetro CCI, se incluyen **2** nuevos fabricantes y su número pasa a **58** en 2021.

Riesgo Bajo	Riesgo Medio	Riesgo Alto	Riesgo Muy Alto
Insulet WECON	N/A	N/A	N/A

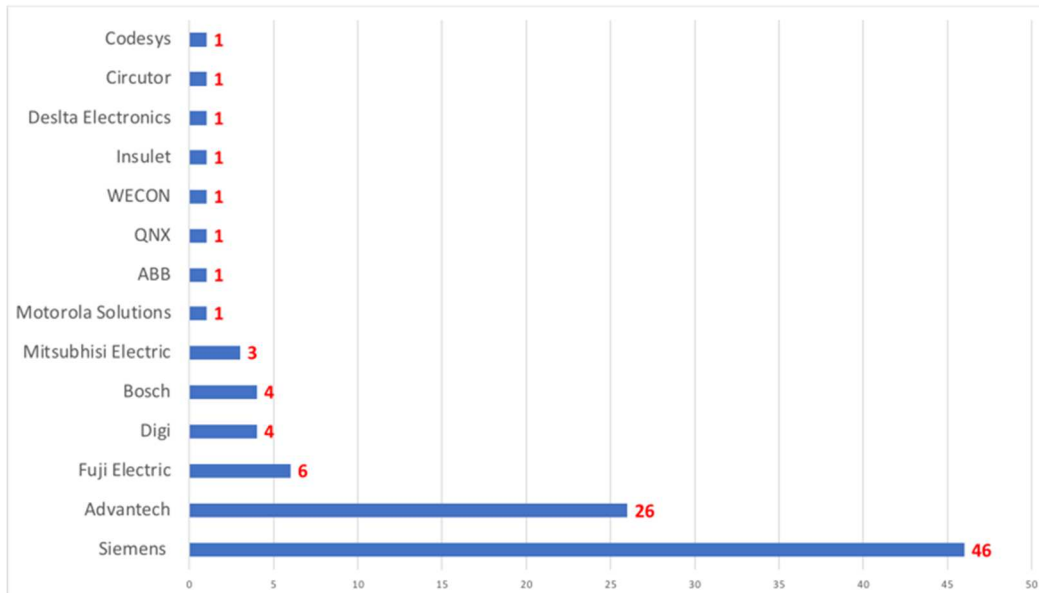
En el caso de **Insulet**, la **debilidad** publicada se asocia a su producto Insulet Omnipod y afecta a todas las versiones debido a la falta de autenticación y autorización en su protocolo de comunicaciones inalámbricas. El ICS-CERT/CISA ha emitido una alerta sobre estas debilidades (**ICSMA-20-079-01**), aunque sus valoraciones CVSS V2 no las cualifican como alertas del termómetro CCI al no impactar en su disponibilidad.

El fabricante **WECON** ve publicada **1 debilidad** que afectan a sus productos LeviStudioU (Versiones 2019-09-21 y anteriores). El ICS-CERT/CISA ha publicado 1 alerta relacionada (**ICSA-21-343-02**), aunque según el criterio del termómetro CCI sobre alertas, no se clasifica como tal.

Nuevas debilidades

El número de vulnerabilidades ICS publicadas y **totalmente caracterizadas** por el NIST desde la última actualización es de **97**.

Una vez más, Siemens destaca entre los fabricantes estudiados:



El detalle de estas debilidades caracterizadas en Diciembre se pueden encontrar en el **ANEXO II**.

Finalizando 2021, podemos constatar que la tendencia en la investigación de debilidades en los sistemas de control utilizados en múltiples sectores, sigue creciendo de manera sostenida.



Nuevas alertas

Este mes, el NIST ha publicado (completamente caracterizadas) **4 nuevas alertas** de fabricante.

Recordamos que se clasifican cómo alertas dado que la explotación de la vulnerabilidad presenta una complejidad baja, tiene cómo vector de acceso la red y puede causar una total pérdida de servicio. (Según la clasificación **CVSS V2**, para permitir la clasificación histórica de debilidades en productos más antiguos).

Siemens ha visto publicada **1 alerta** sobre sus productos **POWER METER SICAM Q100**:



Siemens Power Meter SICAM

CVE	Date published	CVSS V2	Warning	Description
CVE-2021-44165	2021-12-14	9.0		A vulnerability has been identified in POWER METER SICAM Q100 (All versions < V2.41), POWER METER SICAM Q100 (All versions < V2.41), POWER METER SICAM Q100 (All versions < V2.41), POWER METER SICAM Q100 (All versions < V2.41). The affected firmware contains a buffer overflow vulnerability in the web application that could allow a remote attacker with engineer or admin privileges to potentially perform remote code execution.

Circutor vuelve a ver publicada otra alerta sobre uno de sus productos, el concentrador de Smart Meters **CIRCUTOR COMPACT DC-S BASIC**.



Circutor Compact DC-S Basic

CVE	Date published	CVSS V2	Warning	Description
CVE-2021-26777	2021-12-02	10.0		Buffer overflow vulnerability in function SetFirewall in index.cgi in CIRCUTOR COMPACT DC-S BASIC smart metering concentrator Firmware version CIR_CDC_v1.2.17, allows attackers to execute arbitrary code.

Una vez más, esta debilidad se asocia al interfaz Web del dispositivo, no suficientemente protegido ante el tamaño de las entradas de datos (CWE-120). **Circutor** termina 2021 con una exposición al riesgo **Alta** y con un CVSS V2 medio **de 9.0**.

El siguiente fabricantes que ha visto publicada una alerta sobre sus productos es **Digi**. En particular, la debilidad se ha detectado sobre sus productos de comunicaciones TransPort DR64, SR44 VC74, y WR:



Digi TransPort WR

La debilidad está asociada a la debilidad de un protocolo propietario (ZING) que se utiliza para la configuración total de estos dispositivos a través de la red Ethernet.

CVE	Date published	CVSS V2	Warning	Description
CVE-2021-35978	2021-12-10	10.0		An issue was discovered in Digi TransPort DR64, SR44 VC74, and WR. The ZING protocol allows arbitrary remote command execution with SUPER privileges. This allows an attacker (with knowledge of the protocol) to execute arbitrary code on the controller including overwriting firmware, adding/removing users, disabling the internal firewall, etc.

La última alerta publicada, afecta a distintos productos de grabación y reproducción de vídeo de **Bosch**.



CVE	Date published	CVSS V2	Warning	Description
CVE-2021-23862	2021-12-08	9.0		A crafted configuration packet sent by an authenticated administrative user can be used to execute arbitrary commands in system context. This issue also affects installations of the VRM, DIVAR IP, BVMS with VRM installed, the VIDEOJET decoder (VJD-7513 and VJD-8000).

Este fabricante ha acumulado 28 debilidades publicadas en 2021 y presenta un CVSS V2 medio de 5.7 en los últimos 10 años.



Mapa de riesgo

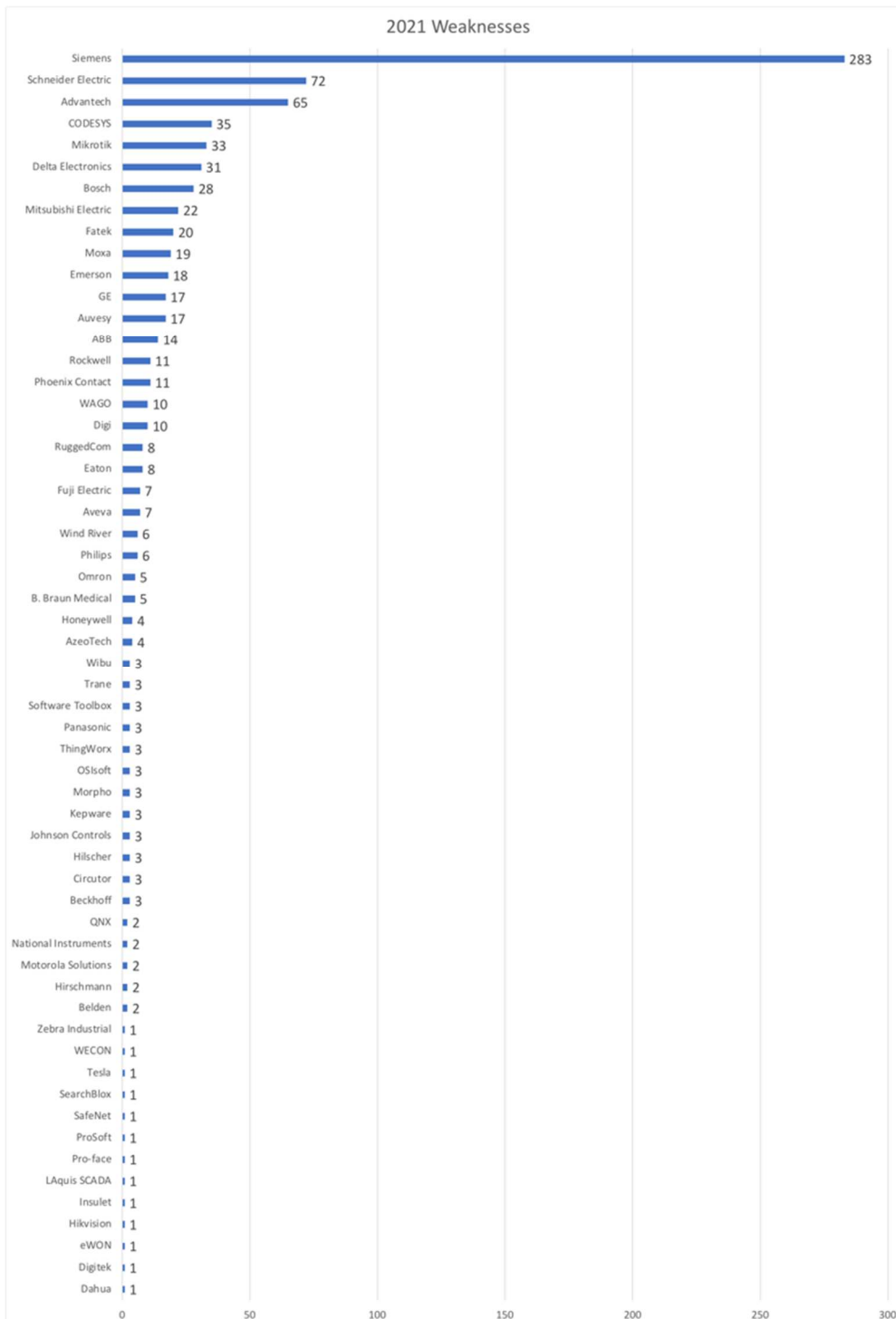
31 de Diciembre de 2021

	Circutor	Dahua		
Digitel Hikvision Johnson Controls Pro-face Zebra Industrial	Advantech Auvesy B. Braun Medical Beckhoff Bosch Delta Electronics Digi Emerson Hilscher Mitsubishi Electric Morpho Moxa Panasonic Phoenix Contact RuggedCom Schneider Electric Wago			Siemens
ABB Belden CODESYS Eaton eWON Fatek Fuji Electric Hirschmann Honeywell Kepware LAquis SCADA Omron PTC (ThingWorx) QNX Rockwell Software Toolbox WECON Wind River	GE Mikrotik			
Aveva Azeotech Insulet Motorola Solutions National Instruments OSIsoft Philips ProSoft SafeNet SearchBlox Tesla Trane Wibu Systems				

Cambios en el riesgo de fabricante

Solamente la inclusión de **WECON** e **Insulet** en el mapa de exposición al riesgo, suponen una novedad.

El resto de los fabricantes mantienen su nivel en el mapa de calor cualitativo de exposición al riesgo y destacan las **283 vulnerabilidades** publicadas por el NIST en 2021 para el fabricante **Siemens**.



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 encuatro rangos: Bajo, Medio, Alto y Muy Alto.

				MUY ALTO
		ALTO		
	MEDIO			
BAJO				

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 como **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.



ANEXO II – Vulnerabilidades publicadas por el NIST desde el último termómetro CCI

CVE	Date published	CVSS	Warning	Description
CVE-2021-44165	2021-12-14	9.0		A vulnerability has been identified in POWER METER SICAM Q100 (All versions < V2.41), POWER METER SICAM Q100 (All versions < V2.41), POWER METER SICAM Q100 (All versions < V2.41). The affected firmware contains a buffer overflow vulnerability in the web application that could allow a remote attacker with engineer or admin privileges to potentially perform remote code execution.
CVE-2021-35978	2021-12-10	10.0		An issue was discovered in Digi TransPort DR64, SR44 VC74, and WR. The ZING protocol allows arbitrary remote command execution with SUPER privileges. This allows an attacker (with knowledge of the protocol) to execute arbitrary code on the controller including overwriting firmware, adding/removing users, disabling the internal firewall, etc.
CVE-2021-23862	2021-12-08	9.0		A crafted configuration packet sent by an authenticated administrative user can be used to execute arbitrary commands in system context. This issue also affects installations of the VRM, DIVAR IP, BVMS with VRM installed, the VIDEOJET decoder (VJD-7513 and VJD-8000).
CVE-2021-26777	2021-12-02	10.0		Buffer overflow vulnerability in function SetFirewall in index.cgi in CIRCUTOR COMPACT DC-S BASIC smart metering concentrator Firmware version CIR_CDC_v1.2.17, allows attackers to execute arbitrary code.
CVE-2021-21916	2021-12-22	7.5		An exploitable SQL injection vulnerability exist in the 'group_list' page of the Advantech R-SeeNet 2.4.15 (30.07.2021). A specially-crafted HTTP request at 'description_filter' parameter. An attacker can make authenticated HTTP requests to trigger this vulnerability. This can be done as any authenticated user or through cross-site request forgery.
CVE-2021-21910	2021-12-22	7.2		A privilege escalation vulnerability exists in the Windows version of installation for Advantech R-SeeNet Advantech R-SeeNet 2.4.15 (30.07.2021). A specially-crafted file can be replaced in the system to escalate privileges to NT SYSTEM authority. An attacker can provide a malicious file to trigger this vulnerability.
CVE-2021-21915	2021-12-22	6.5		An exploitable SQL injection vulnerability exist in the 'group_list' page of the Advantech R-SeeNet 2.4.15 (30.07.2021). A specially-crafted HTTP request at 'company_filter' parameter. An attacker can make authenticated HTTP requests to trigger this vulnerability. This can be done as any authenticated user or through cross-site request forgery.
CVE-2021-21917	2021-12-22	6.5		An exploitable SQL injection vulnerability exist in the 'group_list' page of the Advantech R-SeeNet 2.4.15 (30.07.2021). A specially-crafted HTTP request at 'ord' parameter. An attacker can make authenticated HTTP requests to trigger this vulnerability. This can be done as any authenticated user or through cross-site request forgery.
CVE-2021-21922	2021-12-22	6.5		A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger this vulnerability at 'username_filter' parameter with the administrative account or through cross-site request forgery.
CVE-2021-21920	2021-12-22	6.5		A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger this vulnerability at 'surname_filter' parameter with the administrative account or through cross-site request forgery.
CVE-2021-21918	2021-12-22	6.5		A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger this vulnerability at 'name_filter' parameter. However, the high privilege super-administrator account needs to be used to achieve exploitation without cross-site request forgery attack.
CVE-2021-21921	2021-12-22	6.5		A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger this vulnerability at 'name_filter' parameter with the administrative account or through cross-site request forgery.
CVE-2021-21937	2021-12-22	6.5		A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger this vulnerability at 'host_alt_filter' parameter. This can be done as any authenticated user or through cross-site request forgery.
CVE-2021-21935	2021-12-22	6.5		A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger this vulnerability at 'host_alt_filter2' parameter. This can be done as any authenticated user or through cross-site request forgery.



CVE	Date published	CVSS	Warning	Description
CVE-2021-21936	2021-12-22	6.5		A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger this vulnerability at 'health_alt_filter' parameter. This can be done as any authenticated user or through cross-site request forgery.
CVE-2021-21923	2021-12-22	6.5		A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger this vulnerability at 'company_filter' parameter with the administrative account or through cross-site request forgery.
CVE-2021-21919	2021-12-22	6.5		A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger this vulnerability at 'ord' parameter. However, the high privilege super-administrator account needs to be used to achieve exploitation without cross-site request forgery attack.
CVE-2021-21932	2021-12-22	6.5		A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger this at 'name_filter' parameter. This can be done as any authenticated user or through cross-site request forgery.
CVE-2021-21934	2021-12-22	6.5		A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger this at 'imei_filter' parameter. This can be done as any authenticated user or through cross-site request forgery.
CVE-2021-21933	2021-12-22	6.5		A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger this at 'esn_filter' parameter. This can be done as any authenticated user or through cross-site request forgery.
CVE-2021-21927	2021-12-22	6.5		A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger these vulnerabilities. This can be done as any authenticated user or through cross-site request forgery at 'loc_filter' parameter.
CVE-2021-21925	2021-12-22	6.5		A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger these vulnerabilities. This can be done as any authenticated user or through cross-site request forgery at 'firm_filter' parameter.
CVE-2021-21924	2021-12-22	6.5		A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger these vulnerabilities. This can be done as any authenticated user or through cross-site request forgery at 'desc_filter' parameter.
CVE-2021-21931	2021-12-22	6.5		A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests at 'stat_filter' parameter to trigger this vulnerability. This can be done as any authenticated user or through cross-site request forgery.
CVE-2021-21930	2021-12-22	6.5		A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests at 'sn_filter' parameter to trigger this vulnerability. This can be done as any authenticated user or through cross-site request forgery.
CVE-2021-21929	2021-12-22	6.5		A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests at 'prod_filter' parameter to trigger this vulnerability. This can be done as any authenticated user or through cross-site request forgery.
CVE-2021-21928	2021-12-22	6.5		A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests at 'mac_filter' parameter to trigger this vulnerability. This can be done as any authenticated user or through cross-site request forgery.
CVE-2021-21926	2021-12-22	4.0		A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger these vulnerabilities. This can be done as any authenticated user or through cross-site request forgery at 'health_filter' parameter.
CVE-2021-38401	2021-12-20	6.8		Fuji Electric V-Server Lite and Tellus Lite V-Simulator prior to v4.0.12.0 is vulnerable to an untrusted pointer dereference, which may allow an attacker to execute arbitrary code and cause the application to crash.
CVE-2021-38419	2021-12-20	6.8		Fuji Electric V-Server Lite and Tellus Lite V-Simulator prior to v4.0.12.0 is vulnerable to an out-of-bounds write, which can result in data corruption, a system crash, or code execution.
CVE-2021-38409	2021-12-20	6.8		Fuji Electric V-Server Lite and Tellus Lite V-Simulator prior to v4.0.12.0 is vulnerable to an access of uninitialized pointer, which may allow an attacker read from or write to unexpected memory locations, leading to a denial-of-service.
CVE-2021-38413	2021-12-20	6.8		Fuji Electric V-Server Lite and Tellus Lite V-Simulator prior to v4.0.12.0 is vulnerable to a stack-based buffer overflow, which may allow an attacker to achieve code execution.
CVE-2021-38415	2021-12-20	6.8		Fuji Electric V-Server Lite and Tellus Lite V-Simulator prior to v4.0.12.0 is vulnerable a heap-based buffer overflow when parsing a specially crafted project file, which may allow an attacker to execute arbitrary code.
CVE-2021-38421	2021-12-20	5.8		Fuji Electric V-Server Lite and Tellus Lite V-Simulator prior to v4.0.12.0 is vulnerable to an out-of-bounds read, which may allow an attacker to read sensitive information from other memory locations or cause a crash.
CVE-2021-20608	2021-12-17	5.0		Improper Handling of Length Parameter Inconsistency vulnerability in Mitsubishi Electric GX Works2 versions 1.606G and prior allows a remote unauthenticated attacker to cause a DoS condition in GX Works2 by getting GX Works2 to read a tampered program file from a Mitsubishi Electric PLC by sending malicious crafted packets to tamper with the program file.



CVE	Date published	CVSS	Warning	Description
CVE-2021-20606	2021-12-17	4.3		Out-of-bounds Read vulnerability in Mitsubishi Electric GX Works2 versions 1.606G and prior, MELSOFT Navigator all versions and EZSocket all versions allows an attacker to cause a DoS condition in the software by getting a user to open malicious project file specially crafted by an attacker.
CVE-2021-20607	2021-12-17	4.3		Integer Underflow vulnerability in Mitsubishi Electric GX Works2 versions 1.606G and prior, MELSOFT Navigator all versions and EZSocket all versions allows an attacker to cause a DoS condition in the software by getting a user to open malicious project file specially crafted by an attacker.
CVE-2021-38701	2021-12-15	3.5		Certain Motorola Solutions Avigilon devices allow XSS in the administrative UI. This affects T200/201 before 4.10.0.68; T290 before 4.4.0.80; T008 before 2.2.0.86; T205 before 4.12.0.62; T204 before 3.28.0.166; and T100, T101, T102, and T103 before 2.6.0.180.
CVE-2021-44524	2021-12-14	7.5		A vulnerability has been identified in SiPass integrated V2.76 (All versions), SiPass integrated V2.80 (All versions), SiPass integrated V2.85 (All versions), Siveillance Identity V1.5 (All versions), Siveillance Identity V1.6 (All versions < V1.6.284.0). Affected applications insufficiently limit the access to the internal user authentication service. This could allow an unauthenticated remote attacker to trigger several actions on behalf of valid user accounts.
CVE-2021-42024	2021-12-14	6.8		A vulnerability has been identified in Simcenter STAR-CCM+ Viewer (All versions < 2021.3.1). The starview+.exe application lacks proper validation of user-supplied data when parsing scene files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process.
CVE-2021-44435	2021-12-14	6.8		A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to stack based buffer overflow while parsing specially crafted JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-14903)
CVE-2021-44432	2021-12-14	6.8		A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to stack based buffer overflow while parsing specially crafted JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-14845)
CVE-2021-44440	2021-12-14	6.8		A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to memory corruption condition while parsing specially crafted JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-14912)
CVE-2021-44438	2021-12-14	6.8		A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to an out of bounds write past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14907)
CVE-2021-44437	2021-12-14	6.8		A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to an out of bounds write past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14906)
CVE-2021-44434	2021-12-14	6.8		A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to an out of bounds write past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14902, ZDI-CAN-14866)
CVE-2021-44430	2021-12-14	6.8		A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to an out of bounds write past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14829)
CVE-2021-44439	2021-12-14	6.8		A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to an out of bounds read past the end of an allocated buffer when parsing specially crafted JT files. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-14908)
CVE-2021-44445	2021-12-14	6.8		A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products contains an out of bounds write past the fixed-length heap-based buffer while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-15054)
CVE-2021-44442	2021-12-14	6.8		A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products contains an out of bounds write



CVE	Date published	CVSS	Warning	Description
				past the fixed-length heap-based buffer while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14995)
CVE-2021-44443	2021-12-14	6.8		A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products contains an out of bounds write past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-15039)
CVE-2021-44441	2021-12-14	6.8		A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products contains an out of bounds write past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14913)
CVE-2021-44433	2021-12-14	6.8		A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products contains a use after free vulnerability that could be triggered while parsing specially crafted JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-14900)
CVE-2021-44446	2021-12-14	6.8		A vulnerability has been identified in JT Utilities (All versions < V13.0.3.0), JTTK (All versions < V11.0.3.0). JTTK library in affected products contains an out of bounds write past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14828, ZDI-CAN-14898)
CVE-2021-44447	2021-12-14	6.8		A vulnerability has been identified in JT Utilities (All versions < V13.0.3.0), JTTK (All versions < V11.0.3.0). JTTK library in affected products contains a use-after-free vulnerability that could be triggered while parsing specially crafted JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-14911)
CVE-2021-44450	2021-12-14	6.8		A vulnerability has been identified in JT Utilities (All versions < V12.8.1.1), JTTK (All versions < V10.8.1.1). JTTK library in affected products is vulnerable to an out of bounds read past the end of an allocated buffer when parsing JT files. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-15055, ZDI-CAN-14915, ZDI-CAN-14865)
CVE-2021-44449	2021-12-14	6.8		A vulnerability has been identified in JT Utilities (All versions < V12.8.1.1), JTTK (All versions < V10.8.1.1). JTTK library in affected products contains an out of bounds write past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14830)
CVE-2021-44005	2021-12-14	6.8		A vulnerability has been identified in JT2Go (All versions < V13.2.0.5), Teamcenter Visualization (All versions < V13.2.0.5). The Tiff_Loader.dll contains an out of bounds write past the end of an allocated structure while parsing specially crafted TIFF files. This could allow an attacker to execute code in the context of the current process.
CVE-2021-44002	2021-12-14	6.8		A vulnerability has been identified in JT2Go (All versions < V13.2.0.5), Teamcenter Visualization (All versions < V13.2.0.5). The Jt1001.dll contains an out of bounds write past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-15058)
CVE-2021-44014	2021-12-14	6.8		A vulnerability has been identified in JT2Go (All versions < V13.2.0.5), Teamcenter Visualization (All versions < V13.2.0.5). The Jt1001.dll contains a use-after-free vulnerability that could be triggered while parsing specially crafted JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-15057)
CVE-2021-44001	2021-12-14	6.8		A vulnerability has been identified in JT2Go (All versions < V13.2.0.5), Teamcenter Visualization (All versions < V13.2.0.5). The DL180pdf.dll contains an out of bounds write past the end of an allocated structure while parsing specially crafted PDF files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14974)
CVE-2021-44013	2021-12-14	6.8		A vulnerability has been identified in JT2Go (All versions < V13.2.0.5), Teamcenter Visualization (All versions < V13.2.0.5). The DL180pdf.dll contains an out of bounds write past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-15103)
CVE-2021-41547	2021-12-14	6.5		A vulnerability has been identified in Teamcenter Active Workspace V4.3 (All versions < V4.3.11), Teamcenter Active Workspace V5.0 (All versions < V5.0.10), Teamcenter Active Workspace V5.1 (All versions < V5.1.6), Teamcenter Active Workspace V5.2 (All versions < V5.2.3). The application contains an unsafe unzipping pattern that could lead to a zip path traversal attack. This could allow and attacker to execute a remote shell with admin rights.
CVE-2021-44523	2021-12-14	6.4		A vulnerability has been identified in SiPass integrated V2.76 (All versions), SiPass integrated V2.80 (All versions), SiPass integrated V2.85 (All versions), Siveillance Identity V1.5 (All versions), Siveillance Identity V1.6 (All versions < V1.6.284.0). Affected applications insufficiently limit the access to the internal activity feed database. This



CVE	Date published	CVSS	Warning	Description
				could allow an unauthenticated remote attacker to read, modify or delete activity feed entries.
CVE-2021-42027	2021-12-14	5.8		A vulnerability has been identified in SINUMERIK Edge (All versions < V3.2). The affected software does not properly validate the server certificate when initiating a TLS connection. This could allow an attacker to spoof a trusted entity by interfering in the communication path between the client and the intended server.
CVE-2021-44522	2021-12-14	5.0		A vulnerability has been identified in SiPass integrated V2.76 (All versions), SiPass integrated V2.80 (All versions), SiPass integrated V2.85 (All versions), Siveillance Identity V1.5 (All versions), Siveillance Identity V1.6 (All versions < V1.6.284.0). Affected applications insufficiently limit the access to the internal message broker system. This could allow an unauthenticated remote attacker to subscribe to arbitrary message queues.
CVE-2021-44444	2021-12-14	4.3		A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to an out of bounds read past the end of an allocated buffer when parsing specially crafted JT files. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-15052)
CVE-2021-44436	2021-12-14	4.3		A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to an out of bounds read past the end of an allocated buffer when parsing specially crafted JT files. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-14905)
CVE-2021-44431	2021-12-14	4.3		A vulnerability has been identified in JT Utilities (All versions < V13.1.1.0), JTTK (All versions < V11.1.1.0). JTTK library in affected products is vulnerable to an out of bounds read past the end of an allocated buffer when parsing specially crafted JT files. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-14841)
CVE-2021-44448	2021-12-14	4.3		A vulnerability has been identified in JT Utilities (All versions < V13.0.3.0), JTTK (All versions < V11.0.3.0). JTTK library in affected products is vulnerable to an out of bounds read past the end of an allocated buffer when parsing JT files. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-14843, ZDI-CAN-15051)
CVE-2021-44015	2021-12-14	4.3		A vulnerability has been identified in JT2Go (All versions < V13.2.0.5), Teamcenter Visualization (All versions < V13.2.0.5). The VCRUNTIME140.dll is vulnerable to an out of bounds read past the end of an allocated buffer when parsing specially crafted CGM files. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-15109)
CVE-2021-44003	2021-12-14	4.3		A vulnerability has been identified in JT2Go (All versions < V13.2.0.5), Teamcenter Visualization (All versions < V13.2.0.5). The Tiff_Loader.dll is vulnerable to use of uninitialized memory while parsing user supplied TIFF files. This could allow an attacker to cause a denial-of-service condition.
CVE-2021-44004	2021-12-14	4.3		A vulnerability has been identified in JT2Go (All versions < V13.2.0.5), Teamcenter Visualization (All versions < V13.2.0.5). The Tiff_Loader.dll is vulnerable to an out of bounds read past the end of an allocated buffer when parsing TIFF files. An attacker could leverage this vulnerability to leak information in the context of the current process.
CVE-2021-44007	2021-12-14	4.3		A vulnerability has been identified in JT2Go (All versions < V13.2.0.5), Teamcenter Visualization (All versions < V13.2.0.5). The Tiff_Loader.dll contains an off-by-one error in the heap while parsing specially crafted TIFF files. This could allow an attacker to cause a denial-of-service condition.
CVE-2021-44011	2021-12-14	4.3		A vulnerability has been identified in JT2Go (All versions < V13.2.0.5), Teamcenter Visualization (All versions < V13.2.0.5). The Jt1001.dll is vulnerable to an out of bounds read past the end of an allocated buffer while parsing specially crafted JT files. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-15101)
CVE-2021-44012	2021-12-14	4.3		A vulnerability has been identified in JT2Go (All versions < V13.2.0.5), Teamcenter Visualization (All versions < V13.2.0.5). The Jt1001.dll is vulnerable to an out of bounds read past the end of an allocated buffer when parsing specially crafted JT files. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-15102)
CVE-2021-44017	2021-12-14	4.3		A vulnerability has been identified in JT2Go (All versions < V13.2.0.5), Teamcenter Visualization (All versions < V13.2.0.5). The Image.dll is vulnerable to an out of bounds read past the end of an allocated buffer when parsing specially crafted TIF files. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-15111)
CVE-2021-42022	2021-12-14	3.5		A vulnerability has been identified in SIMATIC eaSie PCS 7 Skill Package (All versions < V21.00 SP3). When downloading files, the affected systems do not properly neutralize



CVE	Date published	CVSS	Warning	Description
				special elements within the pathname. An attacker could then cause the pathname to resolve to a location outside of the restricted directory on the server and read unexpected critical files. The affected file download function is disabled by default.
CVE-2021-42023	2021-12-14	2.1		A vulnerability has been identified in ModelSim Simulation (All versions), Questa Simulation (All versions). The RSA white-box implementation in affected applications insufficiently protects the built-in private keys that are required to decrypt electronic intellectual property (IP) data in accordance with the IEEE 1735 recommended practice. This could allow a sophisticated attacker to discover the keys, bypassing the protection intended by the IEEE 1735 recommended practice.
CVE-2021-22279	2021-12-13	9.3		A Missing Authentication vulnerability in RobotWare for the OmniCore robot controller allows an attacker to read and modify files on the robot controller if the attacker has access to the Connected Services Gateway Ethernet port.
CVE-2021-32024	2021-12-13	7.5		A remote code execution vulnerability in the BMP image codec of BlackBerry QNX SDP version(s) 6.4 to 7.1 could allow an attacker to potentially execute code in the context of the affected process.
CVE-2021-43983	2021-12-13	6.8		WECON LeviStudioU Versions 2019-09-21 and prior are vulnerable to multiple stack-based buffer overflow instances while parsing project files, which may allow an attacker to execute arbitrary code.
CVE-2021-37188	2021-12-10	6.5		An issue was discovered on Digi TransPort devices through 2021-07-21. An authenticated attacker may load customized firmware (because the bootloader does not verify that it is authentic), changing the behavior of the gateway.
CVE-2021-37189	2021-12-10	5.0		An issue was discovered on Digi TransPort Gateway devices through 5.2.13.4. They do not set the Secure attribute for sensitive cookies in HTTPS sessions, which could cause the user agent to send those cookies in cleartext over an HTTP session.
CVE-2021-37187	2021-12-10	4.0		An issue was discovered on Digi TransPort devices through 2021-07-21. An authenticated attacker may read a password file (with reversible passwords) from the device, which allows decoding of other users' passwords.
CVE-2021-43982	2021-12-09	6.8		Delta Electronics CNCSoft Versions 1.01.30 and prior are vulnerable to a stack-based buffer overflow, which may allow an attacker to execute arbitrary code.
CVE-2021-23861	2021-12-08	5.5		By executing a special command, an user with administrative rights can get access to extended debug functionality on the VRM allowing an impact on integrity or availability of the installed software. This issue also affects installations of the DIVAR IP and BVMS with VRM installed.
CVE-2021-23859	2021-12-08	5.0		An unauthenticated attacker is able to send a special HTTP request, that causes a service to crash. In case of a standalone VRM or BVMS with VRM installation this crash also opens the possibility to send further unauthenticated commands to the service. On some products the interface is only local accessible lowering the CVSS base score. For a list of modified CVSS scores, please see the official Bosch Advisory Appendix chapter Modified CVSS Scores for CVE-2021-23859
CVE-2021-23860	2021-12-08	4.3		An error in a page handler of the VRM may lead to a reflected cross site scripting (XSS) in the web-based interface. To exploit this vulnerability an attack must be able to modify the HTTP header that is sent. This issue also affects installations of the DIVAR IP and BVMS with VRM installed.
CVE-2021-34599	2021-12-01	5.8		Affected versions of CODESYS Git in Versions prior to V1.1.0.0 lack certificate validation in HTTPS handshakes. CODESYS Git does not implement certificate validation by default, so it does not verify that the server provides a valid and trusted HTTPS certificate. Since the certificate of the server to which the connection is made is not properly verified, the server connection is vulnerable to a man-in-the-middle attack.
CVE-2020-10627	2021-12-01	4.8		Insulet Omnipod Insulin Management System insulin pump product ID 19191 and 40160 is designed to communicate using a wireless RF with an Insulet manufactured Personal Diabetes Manager device. This wireless RF communication protocol does not properly implement authentication or authorization. An attacker with access to one of the affected insulin pump models may be able to modify and/or intercept data. This vulnerability could also allow attackers to change pump settings and control insulin delivery.
CVE-2021-35533	2021-11-26	7.1		Improper Input Validation vulnerability in the APDU parser in the Bidirectional Communication Interface (BCI) IEC 60870-5-104 function of Hitachi Energy RTU500 series allows an attacker to cause the receiving RTU500 CMU of which the BCI is enabled to reboot when receiving a specially crafted message. By default, BCI IEC 60870-5-104 function is disabled (not configured). This issue affects: Hitachi Energy RTU500 series CMU Firmware version 12.0.* (all versions); CMU Firmware version 12.2.* (all versions); CMU Firmware version 12.4.* (all versions).