

Component group	CPE link	Product	Usage	Link - product details	Link to associated CVEs	# of Vuln encountered	Comments
Remote Terminal Unit (RTU)	https://nvd.nist.gov	Siemens ETA4 Firmware 07 Siemens ETA2 Firmware 11.0	Communication modules used to connect networked industrial components. Includes the energy sector, deployed worldwide		https://nvd.nist.gov	1	So far, the same thing but different version of firmware
	https://nvd.nist.gov	Siemens SICAM AK Siemens SICAM AK 3 Siemens SICAM BC Siemens SICAM BC 1703 Siemens SICAM TM Siemens SICAM TM 1703	An RTU for substation automation: an intelligent automation device specifically designed for the control and monitoring of distribution substations in power grids. It provides comprehensive functionalities for automation, protection, and control of substation equipment	https://www.siemens.com	https://nvd.nist.gov	1	Has been substituted by the SICAM A8000 series
	https://nvd.nist.gov	Siemens SICAM SCC	A service of the affected products listening on all of the host's network interfaces on either port 4884/TCP, 5885/TCP, or port 5886/TCP could allow an attacker to either exfiltrate limited data from the system or to execute code with Microsoft Windows user permissions.	siemens.com/global/en/products/energy/industrial-automation/sicam/sicam-scc	https://nvd.nist.gov	1	
	https://nvd.nist.gov	Siemens SICAM A8000	Is a modular device range for telecontrol and automation applications in all areas of energy supply	https://www.siemens.com/global/en/products/energy/industrial-automation/sicam/sicam-a8000	https://nvd.nist.gov	1	
	https://nvd.nist.gov	Siemens (SICAM Q100) 7KG9501-0AA01-0AA1	It is an RTU. se utiliza para la adquisición, visualización, evaluación y transmisión de variables eléctricas medidas, como tensión, frecuencia, potencia o armónicos. La adquisición, el proceso y la precisión de las variables medidas cumplen la norma de medida de calidad de red IEC 61000-4-30 Clase A	https://mall.industry.siemens.com	https://nvd.nist.gov	1	
	https://nvd.nist.gov	Siemens (SICAM Q100) 7KG9501-0AA31-2AA1	It is an RTU. se utiliza para la adquisición, visualización, evaluación y transmisión de variables eléctricas medidas, como tensión, frecuencia, potencia o armónicos. La adquisición, el proceso y la precisión de las variables medidas cumplen la norma de medida de calidad de red IEC 61000-4-30 Clase A	https://mall.industry.siemens.com	https://nvd.nist.gov	5	

Component group	CPE link	Product	Usage	Link - product details	Link to associated CVEs	# of Vuln encountered	Comments
	https://nvd.nist.gov	Siemens SICAM Toolbox II	Engineering software for SICAM RTUs - provides all functions for integrated and standard engineering throughout the entire plant, e.g.: Data collection, data modeling, configuration, and parameterization. Engineering of process information for the automation and central control-room systems. Administration of the systems and individual parameters of third-party manufacturers	https://www.siemens.com	https://nvd.nist.gov	1	
SCADA	https://nvd.nist.gov	Siemens WinCC 7.4		https://www.siemens.com	https://nvd.nist.gov	2	
	https://nvd.nist.gov	Siemens SIMATIC WinCC Flexible 2008	SCADA		https://nvd.nist.gov	1	
	https://nvd.nist.gov	Siemens SIMATIC WinCC (TIA Portal) 13.0			https://nvd.nist.gov	12	One of the vulnerabilities is the one present in the previous row CPE
	https://nvd.nist.gov	Siemens SIMATIC WinCC 7.4 Service Pack 1 Update 3	SCADA Software	https://new.siemens.com	https://nvd.nist.gov	16	There are a few critical vulnerabilities and the most recent one is from 2022
	https://nvd.nist.gov	Siemens SIMATIC WinAC RTX F 2010 Service Pack 2			https://nvd.nist.gov	2	It coincides with the one from three rows ago, and the other is present in one of the previous Siemens devices as well
	https://nvd.nist.gov	Siemens SIMATIC WinCC Runtime Professional 13 Special Pack 1	Is primarily a software platform for human-machine interface (HMI) and process visualization in industrial automation applications		https://nvd.nist.gov	6	
	https://nvd.nist.gov	Siemens XHQ Server 4.7.1.2; 5.0.0.1	Is a powerful software for operations intelligence with unique capabilities that enables simple access and understanding of complex data. Focusing on process industries challenges, XHQ addresses areas where real-time, relational, and historical data are used, helping users to make more informed decisions – anytime and anywhere.	https://www.siemens.com	https://nvd.nist.gov	1	
	https://nvd.nist.gov	ArcGIS GeoEvent Server ArcGIS GeoEvent Server 10.8.1	It enables organizations to connect to various data streams, such as sensors, IoT devices, social media feeds, and more, and process and analyze the incoming data in real-time	https://enterprise.arcgis.com	https://nvd.nist.gov	1	

Component group	CPE link	Product	Usage	Link - product details	Link to associated CVEs	# of Vuln encountered	Comments
	https://nvd.nist.gov	Ersi ArcGIS Server	Enables organizations to create, manage, and distribute GIS services and applications. It provides the infrastructure for hosting, serving, and managing geospatial data and services			No associated CVEs	
	https://nvd.nist.gov	ESRI ArcGIS ESRI ArcGIS 9.0 ESRI ArcGIS 10.0.2.3200 ESRI ArcGIS 10.1 ESRI ArcGIS 10.2 ESRI ArcGIS 10.8.1 ESRI ArcGIS 11.1	Geospatial platform that provides tools and capabilities for creating, managing, analyzing, and visualizing geographic information		https://nvd.nist.gov	15	There is a total amount of 15 CVEs among the different versions of these products. Not all of them appear in all of the versions
	https://nvd.nist.gov	ESRI ArcGIS 3D Analyst	An extension of the ArcGIS platform that provides advanced capabilities for working with three-dimensional (3D) data			No associated CVEs	
	https://nvd.nist.gov	ESRI ArcGIS ArcSDE	While ArcSDE itself may not be directly used in smart grids, it plays a critical role in enabling the storage, management, and retrieval of geospatial data within the broader ArcGIS system, which can be leveraged in smart grid applications			No associated CVEs	
	https://nvd.nist.gov	ESRI ArcGIS Desktop ESRI ArcGIS Desktop 10.8.1	ArcGIS Desktop is a comprehensive suite of desktop GIS software applications provided by Esri. It includes several key components, such as ArcMap, ArcCatalog, and ArcGIS Pro, which offer powerful tools and functionalities for data visualization, analysis, and geoprocessing	https://www.esri.com	https://nvd.nist.gov	3	
	https://nvd.nist.gov	Esri ArcGIS Earth 1.7.0; 1.8.0; 1.9.0; 1.10.0; 1.10.1; 1.11.0; 1.12.0	Is a lightweight 3D globe viewer developed by Esri that allows users to explore and interact with geospatial data in a three-dimensional environment	https://www.esri.com	https://nvd.nist.gov	1	There version 1.12.0 that does not present any CVEs
	https://nvd.nist.gov	Esri ArcGIS Engine 10.3; 10.4; 10.5; 10.6; 10.7; 10.8; 10.8.1	A developer framework and set of libraries provided by Esri that allows developers to embed geospatial capabilities into custom applications. It provides the core GIS functionality of the ArcGIS platform in a developer-friendly environment		https://nvd.nist.gov	1	

Component group	CPE link	Product	Usage	Link - product details	Link to associated CVEs	# of Vuln encountered	Comments
Geographical Information System (GIS) - Esri	https://nvd.nist.gov	Esri ArcGIS Enterprise Esri ArcGIS Enterprise 10.6.1 Esri ArcGIS Enterprise 10.9	Allows organizations to create, manage, and share geospatial data, maps, and applications within their own infrastructure		https://nvd.nist.gov	3	Version 10.6.1 includes one more CVE and version 10.9 includes one less
	https://nvd.nist.gov	ESRI ArcGIS for Server 10.1.1			https://nvd.nist.gov	3	The CVEs are from 2014
	https://nvd.nist.gov	Esri ArcGIS Online; Esri ArcGIS Online 10.9				No associated CVEs	
	https://nvd.nist.gov	Esri ArcGIS Pro 2.6; 2.6.5; 2.7; 2.7.2; 10.8.1;	Is a powerful desktop GIS application that allows users to create, analyze, and visualize geospatial data in 2D and 3D environments		https://nvd.nist.gov	3	The two versions 2.7.2 and 10.8.1 that do not present any CVEs
	https://nvd.nist.gov	Esri ArcGIS Runtime Toolkit 10.2.0 - 9 for Android & 100.5-10.0				No associated CVEs	A total of 17 products are included in this group
	https://nvd.nist.gov	Esri ArcGIS Server Esri ArcGIS Server 10.2.2 Esri ArcGIS Server 10.3 Esri ArcGIS Server 10.4 Esri ArcGIS Server 10.4.1 Esri ArcGIS Server 10.5 Esri ArcGIS Server 10.6 Esri ArcGIS Server 10.7 Esri ArcGIS Server 10.7.1 Esri ArcGIS Server 10.8 Esri ArcGIS Server 10.8.1 Esri ArcGIS Server 10.9.0 Esri ArcGIS Server on X64 Esri ArcGIS Server 10.6.1 on X64 Esri ArcGIS Server 10.7.1 on X64 Esri ArcGIS Server 10.8.1 on X64 Esri ArcGIS Server 10.9.0 on X64 Esri ArcGIS Server 10.9.1 on X64	Is a component of the Esri ArcGIS platform that allows organizations to publish, share, and manage geospatial services over the web		https://nvd.nist.gov	18	It goes, in some versions, up to 16 CVEs, and the most recent versions only present 6
	https://nvd.nist.gov	ESRI ArcGIS Spatial Analyst	Advanced spatial modeling and analysis tools. It helps with modeling terrains, finding suitable locations and routes, discovering spatial patterns, and performing hydrologic and statistical analysis	https://www.esri.com		No associated CVEs	

Component group	CPE link	Product	Usage	Link - product details	Link to associated CVEs	# of Vuln encountered	Comments
	https://nvd.nist.gov	Esri Portal For Arcgis Esri Portal For Arcgis 10.6 Esri Portal For Arcgis 10.6.1 Esri Portal For Arcgis 10.7.1 Esri Portal For Arcgis 10.8 Esri Portal For Arcgis 10.8.1 Esri Portal For Arcgis 10.8.1 on x64 Esri Portal For Arcgis 10.9 Esri Portal For Arcgis 10.9.1 Esri Portal For Arcgis 10.9.1 on x64 Esri Portal For Arcgis 11.0	A component of the ArcGIS Enterprise platform that allows organizations to create and share geospatial content, maps, and applications within their own secure environment	https://enterprise.arcgis.com	https://nvd.nist.gov	35	There are some of the versions that present up to 26 CVE. The latter versions present less CVEs
	https://nvd.nist.gov	Siemens SICAM PAS (Power Automation System)	SICAM PAS (Power Automation System) meets all the demands placed on a distributed substation control system – both now and in the future. Amongst many other standardized communication protocols, SICAM PAS particularly supports the IEC 61850 standard for communication between substations and IEDs	https://www.siemens.com	https://nvd.nist.gov	8	The affected versions have already been superseded by newer versions
	https://nvd.nist.gov	Siemens SICAM PQS	Stands for SICAM Power Quality System. It is a comprehensive solution offered by Siemens for power quality monitoring and analysis. The SICAM PQS is designed to help utilities, industrial facilities, and other power consumers assess and manage power quality parameters in their electrical networks.	https://mall.industry.siemens.com	https://nvd.nist.gov	2	The affected versions have already been superseded by newer versions
	https://nvd.nist.gov	Siemens SIMATIC S7-1500 Software Controller	The S7-1500 Software Controller can be utilized for control and automation purposes. It can manage and monitor different aspects of the grid, such as power generation, load balancing, voltage regulation, and fault detection. The software controller can execute control algorithms, perform real-time monitoring of grid parameters, and communicate with other devices within the grid infrastructure.	https://opcfoundation.org	https://nvd.nist.gov	10	
	https://nvd.nist.gov	Siemens SINAMICS G120	A versatile and modular drive system that provides motor control capabilities for various industrial applications, including those within the power and energy sector.	https://www.siemens.com	https://nvd.nist.gov	3	

Component group	CPE link	Product	Usage	Link - product details	Link to associated CVEs	# of Vuln encountered	Comments
Power Automation System (PAS)	https://nvd.nist.gov	Siemens SINAMICS G120 (C/P/D) PN	(DERs) can be utilized in various applications within the grid infrastructure. They can be employed in controlling motors in substation equipment, renewable energy systems (such as wind turbines and solar farms), energy storage systems, and other distributed energy resources		https://nvd.nist.gov	1	
	https://nvd.nist.gov	Siemens SINAMICS G120 (C/P/D) W. PN	(DERs) can be utilized in various applications within the grid infrastructure. They can be employed in controlling motors in substation equipment, renewable energy systems (such as wind turbines and solar farms), energy storage systems, and other distributed energy resources		https://nvd.nist.gov	1	
	https://nvd.nist.gov	Siemens SICAM PQ ANALYZER	Power quality analysis. provides comprehensive evaluation options for archived PQ measuring data and fault records. In addition to clearly structured fault record analysis, the fault locator facilitates and accelerates the elimination of faults in the power network	https://www.siemens.com	https://nvd.nist.gov	2	
	https://nvd.nist.gov	ABB zenon 7.50 ABB zenon 7.60 ABB zenon 8.00 ABB zenon 8.10 ABB zenon 8.20	Fulfills the role of a seamless integrator of diverse devices such as ABB and 3rd party make protection relays, meters, substation equipment condition monitoring units, Programmable Logic Controllers (PLC) and Remote Terminal Units (RTUs), deployed in digital electrification solutions It falls more under the control and monitoring systems	https://new.abb.com	https://nvd.nist.gov	7	
	https://nvd.nist.gov	Siemens SIGUARD DSA 4.2 Siemens SIGUARD DSA 4.3 Siemens SIGUARD DSA 4.4	Dynamic security assessment software for real-time and operational planning use. It serves to increase situational awareness and prevent blackouts.	https://www.siemens.com	https://nvd.nist.gov	2	It was found while looking for Demand-Side Management (DSM)
	https://nvd.nist.gov	Siemens SICAM MMU Siemens SICAM SGU Siemens SICAM T Siemens SICAM SGU Firmware	Is a digital measurement transducer that allows the measuring of electrical quantities in electrical networks in a single unit.	https://www.siemens.com	https://nvd.nist.gov	9	There are many CVEs, some of them critical and all of them from 2020

Component group	CPE link	Product	Usage	Link - product details	Link to associated CVEs	# of Vuln encountered	Comments
Advanced Metering Infrastructure (AMI)	https://nvd.nist.gov	Siemens SICAM GridEdge Essential ARM Edition Siemens SICAM GridEdge Essential GDS ARM Edition Siemens SICAM GridEdge Essential GDS Intel Edition Siemens SICAM GridEdge Essential Intel Edition	SICAM GridEdge enables your existing IEC61850 equipment with IoT functionality using just a few clicks. Based on international standards (MQTT, OPC UA Pub/Sub (IEC 62451), IEC61850) data collected from your equipment is transmitted to well-known cloud platforms	https://mall.industry	https://nvd.nist.gov	4	All CVEs are from 2022 and one of them is critical
	https://nvd.nist.gov	Siemens SICAM GridEdge Essential ARM Siemens SICAM GridEdge Essential GDS ARM	SICAM GridEdge enables your existing IEC61850 equipment with IoT functionality using just a few clicks. Based on international standards (MQTT, OPC UA Pub/Sub (IEC 62451), IEC61850) data collected from your equipment is transmitted to well-known cloud platforms	https://mall.industry	https://nvd.nist.gov	1	From 2022
	https://nvd.nist.gov	ABB RER620 - ABB RER620 FIRMWARE ABB SMU615 - ABB SMU615 FIRMWARE	It is designed to automatically interrupt and restore electrical power in the event of a temporary fault or disturbance on the distribution line.	https://new.abb.com	https://nvd.nist.gov	1	Smart meters and data concentrators: Metering Infrastructure
	https://nvd.nist.gov	Siemens EnergyIP 8.5 Siemens EnergyIP 8.6 Siemens EnergyIP 8.7 Siemens EnergyIP 9.0	It is designed to enable utilities and energy companies to manage and optimize their operations, facilitate data management, and support various energy-related applications	https://assets.new.s	https://nvd.nist.gov	2	Shared with DRS
Demand Response Systems (DRS)	https://nvd.nist.gov	Siemens EnergyIP 8.5 Siemens EnergyIP 8.6 Siemens EnergyIP 8.7 Siemens EnergyIP 9.0	It is designed to enable utilities and energy companies to manage and optimize their operations, facilitate data management, and support various energy-related applications. It is also used in the Demand Response field of the smart grid.	https://assets.new.s	https://nvd.nist.gov	2	Shared with PAS
	https://nvd.nist.gov	Siemens SIMATIC S7 300 CPU Siemens SIMATIC S7 400 CPU	It is a PLC used for many things and widely deployed. It could be used for smart grids	https://www.siemens	https://nvd.nist.gov	2	They are both from 2016
	https://nvd.nist.gov	Siemens SIMATIC ET 200SP Open Controller	It combines the functionality of a PLC with the openness of a PC-based system, allowing for flexible programming and communication capabilities	https://www.siemens	https://nvd.nist.gov	2	

Component group	CPE link	Product	Usage	Link - product details	Link to associated CVEs	# of Vuln encountered	Comments
Programmable Logic Controller (PLC)	https://nvd.nist.gov	Siemens S7-1200 CPU 1211C; 1212C 1212f 1214C 1214fc 1215C 1215fc 1217c	PLCs: the intelligent choice for compact automation solutions with extended communication options and integrated technology functions.	https://www.siemens.com	https://nvd.nist.gov	1	
	https://nvd.nist.gov	Siemens SIMATIC S7-1200 CPU 12 1211C Siemens SIMATIC S7-1200 CPU 12 1212C Siemens SIMATIC S7-1200 CPU 12 1212fc Siemens SIMATIC S7-1200 CPU 12 1214C Siemens SIMATIC S7-1200 CPU 12 1214fc Siemens SIMATIC S7-1200 CPU 12 1215C Siemens SIMATIC S7-1200 CPU 12 1215fc Siemens SIMATIC S7-1200 CPU 12 1217C	It is a PLC used for many things and widely deployed. It could be used for smart grids, it is mostly created for smaller infrastructures though	https://www.siemens.com	https://nvd.nist.gov	6	They are from 2021 and 2022
	https://nvd.nist.gov	Siemens SIMATIC S7-1500 CPU	It is a PLC . In the context of smart grids, the SIMATIC S7-1500 CPU can be employed for control, monitoring, and automation purposes. It serves as a central processing unit that executes control algorithms and manages the operation of the grid infrastructure. The CPU communicates with other devices, such as sensors, actuators, and communication networks, to enable real-time monitoring and control of power generation, transmission, and distribution systems.	https://www.siemens.com	https://nvd.nist.gov	3	