CPE product affected	CVE id	CVE link	CVSS - vector and score	CIA	Description of the vulnerability	What could an attacker achieve?	Capabilities
ESRI ArcGIS 9.0	CVE-2005-1394	https://nvd.nist.gov/vuln/detail/CVE-2005-1394	AV:L/AC:L/Au:N/C:C/I:C/A:C **7,2 HIGH**	HIGH;HIGH;HIGH	Format string vulnerability	allows local users to gain privileges via format string specifiers in the ARCHOME environment variable to (1) wservice or (2) lockmgr	LATERAL MOVEMENT / PRIVILEGE ESCALATION
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	CVE-2007-4278	https://nvd.nist.gov/vuln/detail/CVE-2007-4278	AV:N/AC:L/Au:N/C:L/I:L/A:L **7,5 HIGH**	LOW;LOW;LOW	Improper Restriction of Operations within the Bounds of a Memory Buffer	allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a large number that requires more than 8 bytes to represent in ASCII, which triggers the overflow in an sprintf function call.	COMMAND INJECTION DENIAL OF SERVICE
Siemens SIMATIC WinCC 7.4 Service Pack 1 Update 3	CVE-2010-2772	https://nvd.nist.gov/vuln/detail/CVE-2010-2772	AV:N/AC:L/PR:N/UI:N/S:C/C:H/I: H/A:H **10,0 CRITICAL**	HIGH;HIGH;HIGH	Credentials Management Errors	uses a hard-coded password, which allows local users to access a back-end database and gain privileges, as demonstrated in the wild in July 2010 by the Stuxnet worm	EAVESDROPPING LATERAL MOVEMENT / PRIVILEGE ESCALATION
ESRI ArcGIS ESRI ArcGIS 9.0 ESRI ArcGIS 10.0.2.3200	CVE-2012-1661	https://nvd.nist.gov/vuln/detail/CVE-2012-1661	AV:N/AC:M/Au:N/C:C/I:C/A:C **9,3 HIGH**	HIGH;HIGH;HIGH	Improper Control of Generation of Code ('Code Injection') - does not properly prompt users before executing embedded VBA macros	allows user-assisted remote attackers to execute arbitrary VBA code via a crafted map (. mxd) file	COMMAND INJECTION
ESRI ArcGIS 10.1	CVE-2012-4949	https://nvd.nist.gov/vuln/detail/CVE-2012-4949	AV:N/AC:L/Au:S/C:P/I:P/A:P **6,5 MEDIUM**	LOW;LOW;LOW	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	allows remote authenticated users to execute arbitrary SQL commands via the where parameter to a query URI for a REST service.	COMMAND INJECTION
ESRI ArcGIS 10.1	CVE-2013-5221	https://nvd.nist.gov/vuln/detail/CVE-2013-5221	AV:N/AC:M/Au:S/C:N/I:P/A:N **3,5 LOW**	none;LOW;none	Improper Input Validation	allows remote authenticated users to upload .exe files by leveraging (1) publisher or (2) administrator privileges.	COMMAND INJECTION
ESRI ArcGIS 10.1	CVE-2013-5222	https://nvd.nist.gov/vuln/detail/CVE-2013-5222	AV:N/AC:M/Au:S/C:N/I:P/A:N **3,5 LOW**	none;LOW;none	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	allow remote authenticated users to inject arbitrary web script or HTML via unspecified vectors.	COMMAND INJECTION
Siemens SINAMICS G120	CVE-2013-6920	https://nvd.nist.gov/vuln/detail/CVE-2013-6920	AV:N/AC:L/PR:N/UI:N/S:C/C:H/I: H/A:H **10,0 CRITICAL**	HIGH;HIGH;HIGH	Improper Authentication - do not require authentication for FTP and TELNET sessions	allows remote attackers to bypass intended access restrictions via TCP traffic to port (1) 21 or (2) 23.	ACCESS
ESRI ArcGIS 10.1 ESRI ArcGIS 10.2	CVE-2013-7231	https://nvd.nist.gov/vuln/detail/CVE-2013-7231	AV:N/AC:M/Au:S/C:N/I:P/A:N **3,5 LOW**	none;LOW;none	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors	COMMAND INJECTION

ESRI ArcGIS ESRI ArcGIS 9.0 ESRI ArcGIS 10.0.2.3200 ESRI ArcGIS 10.1 ESRI ArcGIS 10.2	CVE-2013-7232	https://nvd.nist.gov/vuln/detail/CVE-2013-7232	AV:N/AC:L/Au:N/C:P/I:P/A:P **7,5 HIGH**	LOW;LOW;LOW	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	allows remote attackers to execute arbitrary SQL commands via unspecified input to the map or feature service.	COMMAND INJECTION FALSE DATA INJECTION EAVESDROPPING
ESRI ArcGIS for Server 10.1.1	CVE-2014-5121	https://nvd.nist.gov/vuln/detail/CVE-2014-5121	AV:N/AC:M/Au:N/C:N/I:P/A:N **4,3 MEDIUM**	none;LOW;none	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	allow remote attackers to inject arbitrary web script or HTML via unspecified parameters.	COMMAND INJECTION
ESRI ArcGIS for Server 10.1.1	CVE-2014-5122	https://nvd.nist.gov/vuln/detail/CVE-2014-5122	AV:N/AC:M/Au:N/C:P/I:P/A:N **5,8 MEDIUM**	LOW;LOW;none	Open redirect vulnerability	allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via an unspecified parameter, related to login.	OTHER
ESRI ArcGIS for Server 10.1.1	CVE-2014-9741	https://nvd.nist.gov/vuln/detail/CVE-2014-9741	AV:N/AC:M/Au:N/C:N/I:P/A:N **4,3 MEDIUM**	none;LOW;none	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	allow remote attackers to inject arbitrary web script or HTML via unspecified vectors.	COMMAND INJECTION
SIPROTEC	CVE-2015-5374	https://nvd.nist.gov/vuln/detail/CVE-2015-5374	AV:N/AC:L/Au:N/C:N/I:N/A:C **7,8 HIGH**	none;none;HIGH	Data Processing Errors	Specially crafted packets sent to port 50000/UDP could cause a denial-of-service of the affected device. A manual reboot may be required to recover the service of the device.	DENIAL OF SERVICE
SIPROTEC	CVE-2016-4784	https://nvd.nist.gov/vuln/detail/CVE-2016-4784	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I: N/A:N **5,3 MEDIUM**	LOW;none;none	Exposure of Sensitive Information to an Unauthorized Actor	could allow remote attackers to obtain sensitive device information if network access was obtained.	EAVESDROPPING
SIPROTEC	CVE-2016-4785	https://nvd.nist.gov/vuln/detail/CVE-2016-4785	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I: N/A:N **5,3 MEDIUM**	LOW;none;none	Exposure of Sensitive Information to an Unauthorized Actor	could allow remote attackers to obtain a limited amount of device memory content if network access was obtained	EAVESDROPPING
Siemens SIMATIC WinCC 7.4 Service Pack 1 Update 3	CVE-2016-5743	https://nvd.nist.gov/vuln/detail/CVE-2016-5743	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I: H/A:H **9,8 CRITICAL**	HIGH;HIGH;HIGH	Improper Input Validation	allow remote attackers to execute arbitrary code via crafted packets.	COMMAND INJECTION
Siemens SICAM PAS (Power Automation System)	CVE-2016-5848	https://nvd.nist.gov/vuln/detail/CVE-2016-5848	AV:L/AC:L/PR:H/UI:N/S:U/C:H/I: H/A:H	HIGH;HIGH;HIGH	Exposure of Sensitive Information to an Unauthorized Actor & Credential Management Errors - does not properly restrict password data in the database	makes it easier for local users to calculate passwords by leveraging unspecified database privileges.	LATERAL MOVEMENT / PRIVILEGE ESCALATION
Siemens SICAM PAS (Power Automation System)	CVE-2016-5849	https://nvd.nist.gov/vuln/detail/CVE-2016-5849	AV:L/AC:H/PR:L/UI:N/S:U/C:L/I: N/A:N	LOW;none;none	Exposure of Sensitive Information to an Unauthorized Actor	allows local users to obtain sensitive configuration information by leveraging database stoppage.	EAVESDROPPING

SIPROTEC	CVE-2016-7112	https://nvd.nist.gov/vuln/detail/CVE-2016-7112	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I: H/A:H **9,8 CRITICAL**	HIGH;HIGH;HIGH	Improper Authentication	could possibly circumvent authentication and perform certain administrative operations.	LATERAL MOVEMENT / PRIVILEGE ESCALATION
SIPROTEC	CVE-2016-7113	https://nvd.nist.gov/vuln/detail/CVE-2016-7113	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I: N/A:H **7,5 HIGH**	none;none;HIGH	Resource Management Errors	Specially crafted packets sent to port 80/tcp could cause the affected device to go into defect mode.	DENIAL OF SERVICE
SIPROTEC	CVE-2016-7114	https://nvd.nist.gov/vuln/detail/CVE-2016-7114	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I: H/A:H **8,8 HIGH**	HIGH;HIGH;HIGH	Improper Authentication	could possibly circumvent authentication and perform certain administrative operations. A legitimate user must be logged into the web interface for the attack to be successful.	ACCESS
Siemens SIMATIC WinCC 7.4 Service Pack 1 Update 3 —————— Siemens SIMATIC WinAC RTX F 2010 Service Pack 2	CVE-2016-7165	https://nvd.nist.gov/vuln/detail/CVE-2016-7165	AV:L/AC:H/PR:H/UI:N/S:U/C:H/I: H/A:H **6,4 MEDIUM**	HIGH;HIGH;HIGH	Improper Access Control - Unquoted service paths could allow local Microsoft Windows operating system users to escalate their privileges if the affected products are not installed under their default path ("C:\Program Files*" or the localized equivalent).	By scalating privileges, an attacker could have more understanding of the network and move laterally inside the network, therefore infecting other systems	EAVESDROPPING LATERAL MOVEMENT / PRIVILEGE ESCALATION
Siemens ETA4 Firmware 07 and 11.0 Siemens SICAM TM ; TM 1703 Siemens SICAM AK ; AK 3 Siemens SICAM BC; BC 1703 Siemens SICAM AK Siemens SICAM AK 3 Siemens SICAM BC Siemens SICAM BC 1703 Siemens SICAM TM Siemens SICAM TM 1703	CVE-2016-7987	https://nvd.nist.gov/vuln/detail/CVE-2016-7987	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I: N/A:H **7,5 HIGH**	none;none;HIGH	Specially crafted packets sent to Port 2404/TCP could cause the affected device to go into defect mode. A cold start might be required to recover the system, a Denial-of-Service Vulnerability	a Denial of Service of the application	DENIAL OF SERVICE
Siemens SICAM PAS (Power Automation System)	CVE-2016-8566	https://nvd.nist.gov/vuln/detail/CVE-2016-8566	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I: H/A:H	HIGH;HIGH;HIGH	Credentials Management Errors - Storing Passwords in a Recoverable Format	an authenticated local attacker with certain privileges could possibly reconstruct the passwords of users for accessing the database.	LATERAL MOVEMENT / PRIVILEGE ESCALATION
Siemens SICAM PAS (Power Automation System)	CVE-2016-8567	https://nvd.nist.gov/vuln/detail/CVE-2016-8567	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I: H/A:H	HIGH;HIGH;HIGH	Use of Hard-coded Credentials - factory account with hard-coded passwords is present	Attackers might gain privileged access to the database over Port 2638/TCP.	FALSE DATA INJECTION EAVESDROPPING
Siemens SIMATIC S7 300 CPU Siemens SIMATIC S7 400 CPU	CVE-2016-8672	https://nvd.nist.gov/vuln/detail/CVE-2016-8672	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I: N/A:N **5,3 MEDIUM**	LOW;none;none	Exposure of Sensitive Information to an Unauthorized Actor - The integrated web server delivers cookies without the "secure" flag	Could get access to conficential information	EAVESDROPPING

Siemens SIMATIC S7 300 CPU Siemens SIMATIC S7 400 CPU	CVE-2016-8673	https://nvd.nist.gov/vuln/detail/CVE-2016-8673	AV:N/AC:L/PR:N/UI:R/S:U/C:H/I: H/A:H **8,8 HIGH**	HIGH;HIGH;HIGH	Cross-Site Request Forgery (CSRF)	could allow remote attackers to perform actions with the permissions of an authenticated user, provided the targeted user has an active session and is induced to trigger the malicious request	COMMAND INJECTION
Siemens SICAM PAS (Power Automation System)	CVE-2016-9156	https://nvd.nist.gov/vuln/detail/CVE-2016-9156	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I: L/A:L	LOW;LOW;LOW	Improper Access Control	could allow a remote attacker to upload, download, or delete files in certain parts of the file system by sending specially crafted packets to port 19235/TCP	FALSE DATA INJECTION EAVESDROPPING
Siemens SICAM PAS (Power Automation System)	CVE-2016-9157	https://nvd.nist.gov/vuln/detail/CVE-2016-9157	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I: H/A:H	HIGH;HIGH;HIGH	Improper Input Validation	could allow a remote attacker to cause a Denial of Service condition and potentially lead to unauthenticated remote code execution by sending specially crafted packets to port 19234/TCP	COMMAND INJECTION DENIAL OF SERVICE
Siemens WinCC 7.4	CVE-2017-12069	https://nvd.nist.gov/vuln/detail/CVE-2017-12069	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I: N/A:H **8,2 HIGH**	LOW;none;HIGH	Improper Restriction of XML External Entity Reference	By sending specially crafted packets to the OPC Discovery Server at port 4840/tcp, an attacker might cause the system to access various resources chosen by the attacker.	DENIAL OF SERVICE
Siemens SINAMICS G120 (C/P/D) W. PN	CVE-2017-2680	https://nvd.nist.gov/vuln/detail/CVE-2017-2680	AV:A/AC:L/PR:N/UI:N/S:U/C:N/I: N/A:H **6,5 MEDIUM**	none;none;HIGH	Uncontrolled Resource Consumption	Specially crafted PROFINET DCP broadcast packets could cause a denial of service condition of affected products on a local Ethernet segment (Layer 2). Human interaction is required to recover the systems	DENIAL OF SERVICE
Siemens SIMATIC S7-1500 Software Controller -------------------- Siemens SINAMICS G120 (C/P/D) PN	CVE-2017-2681	https://nvd.nist.gov/vuln/detail/CVE-2017-2681	AV:A/AC:L/PR:N/UI:N/S:U/C:N/I: N/A:H **6,5 MEDIUM**	none;none;HIGH	Uncontrolled Resource Consumption	could cause a denial of service	DENIAL OF SERVICE

Siemens SIMATIC WinCC Flexible 2008 —————— Siemens SIMATIC WinCC (TIA Portal) 13.0 —————— Siemens SIMATIC WinAC RTX F 2010 Service Pack 2	CVE-2017-6865	https://nvd.nist.gov/vuln/detail/CVE-2017-6865	AV:A/AC:L/PR:N/UI:N/S:U/C:N/I: N/A:H **6,5 MEDIUM**	none;none;HIGH	Improper Input Validation	Specially crafted PROFINET DCP broadcast packets sent to the affected products on a local Ethernet segment (Layer 2) could cause a Denial-of-Service condition of some services. The services require manual restart to recover.	DENIAL OF SERVICE
Siemens XHQ Server 4.7.1.2; 5.0.0.1	CVE-2017-6866	https://nvd.nist.gov/vuln/detail/CVE-2017-6866	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I: N/A:N **6,5 MEDIUM**	HIGH;none;none	Improper Access Control vulnerability	Could allow a low privilege user to gain reading access compromising this way the confidentiality	EAVESDROPPING
Siemens SIMATIC WinCC 7.4 Service Pack 1 Update 3	CVE-2017-6867	https://nvd.nist.gov/vuln/detail/CVE-2017-6867	AV:N/AC:L/PR:H/UI:N/S:U/C:N/I: N/A:H **4,9 MEDIUM**	none;none;HIGH	Improper Input Validation	could allow an authenticated, remote attacker who is member of the "administrators" group to crash services by sending specially crafted messages to the DCOM interface.	DENIAL OF SERVICE
SIPROTEC	CVE-2018-11451	https://nvd.nist.gov/vuln/detail/CVE-2018-11451	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I: N/A:H **7,5 HIGH**	none;none;HIGH	Improper Input Validation - Specially crafted packets to port 102/tcp could cause a denial-of- service condition in the affected products	could allow causing a Denial-of-Service condition of the network functionality of the device, compromising the availability of the system A manual restart is required to recover the EN100 module functionality of the affected devices	DENIAL OF SERVICE
Siemens SIMATIC WinCC (TIA Portal) 13.0	CVE-2018-11453	https://nvd.nist.gov/vuln/detail/CVE-2018-11453	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I: H/A:H **7,8 HIGH**	HIGH;HIGH;HIGH	Incorrect Default Permissions - Improper file permissions in the default installation of TIA Portal	may allow an attacker with local file system access to insert specially crafted files which may prevent TIA Portal startup (Denial-of-Service) or lead to local code execution.	COMMAND INJECTION DENIAL OF SERVICE
Siemens SIMATIC WinCC (TIA Portal) 13.0	CVE-2018-11454	https://nvd.nist.gov/vuln/detail/CVE-2018-11454	AV:L/AC:L/PR:N/UI:R/S:C/C:H/I: H/A:H **8,6 HIGH**	HIGH;HIGH;HIGH	Incorrect Default Permissions - Improper file permissions in the default installation of TIA Portal	may allow an attacker with local file system access to manipulate resources which may be transferred to devices and executed there by a different user.	LATERAL MOVEMENT / PRIVILEGE ESCALATION

Siemens SIMATIC WinCC (TIA Portal) 13.0	CVE-2018-13812	https://nvd.nist.gov/vuln/detail/CVE-2018-13812	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I: N/A:N **7,5 HIGH**	HIGH;none;none	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	A directory traversal vulnerability could allow to download arbitrary files from the device. The security vulnerability could be exploited by an attacker with network access to the integrated web server.	EAVESDROPPING
Siemens SIMATIC WinCC (TIA Portal) 13.0	CVE-2018-13813	https://nvd.nist.gov/vuln/detail/CVE-2018-13813	AV:N/AC:L/PR:N/UI:R/S:U/C:H/I: H/A:N **8,1 HIGH**	HIGH;HIGH;none	URL Redirection to Untrusted Site ('Open Redirect') - The webserver of affected HMI devices may allow URL redirections to untrusted websites	The webserver of affected HMI devices may allow URL redirections to untrusted websites. An attacker must trick a valid user who is authenticated to the device into clicking on a malicious link to exploit the vulnerability, and then carry out other attacks.	OTHER
Siemens SIMATIC WinCC (TIA Portal) 13.0	CVE-2018-13814	https://nvd.nist.gov/vuln/detail/CVE-2018-13814	AV:N/AC:L/PR:N/UI:R/S:U/C:H/I: H/A:H **8,8 HIGH**	HIGH;HIGH;HIGH	Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting') - The integrated web server (port 80/tcp and port 443/tcp) of the affected devices could allow an attacker to inject HTTP headers.	An attacker must trick a valid user who is authenticated to the device into clicking on a malicious link to exploit the vulnerability.	OTHER
SIPROTEC	CVE-2018-16563	https://nvd.nist.gov/vuln/detail/CVE-2018-16563	AV:N/AC:H/PR:N/UI:N/S:U/C:N/I: N/A:H **5,9 MEDIUM**	none;none;HIGH	Specially crafted packets to port 102/tcp could cause a denial-of-service condition in the affected products	could allow causing a Denial-of-Service condition of the network functionality of the device, compromising the availability of the system A manual restart is required to recover the EN100 module functionality of the affected devices	DENIAL OF SERVICE
Siemens SIMATIC WinCC 7.4 Service Pack 1 Update 3	CVE-2018-4832	https://nvd.nist.gov/vuln/detail/CVE-2018-4832	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I: N/A:H **7,5 HIGH**	none;none;HIGH	Improper Input Validation	Specially crafted messages sent to the RPC service of the affected products could cause a Denial-of-Service condition on the remote and local communication functionality of the affected products. A reboot of the system is required to recover the remote and local communication functionality.	DENIAL OF SERVICE

SIPROTEC	CVE-2018-4839	https://nvd.nist.gov/vuln/detail/CVE-2018-4839	AV:N/AC:H/PR:L/UI:N/S:U/C:H/I: N/A:N **5,3 MEDIUM**	HIGH;none;none	Inadequate Encryption Strength	An attacker with local access to the engineering system or in a privileged network position and able to obtain certain network traffic could possibly reconstruct access authorization passwords.	LATERAL MOVEMENT / PRIVILEGE ESCALATION
Siemens SICAM SCC —————— Siemens SICAM PQ ANALYZER	CVE-2018-4858	https://nvd.nist.gov/vuln/detail/CVE-2018-4858	AV:L/AC:L/PR:N/UI:R/S:U/C:H/I: H/A:H **7,8 HIGH**	HIGH;HIGH;HIGH	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	Successful exploitation requires an attacker to be able to send a specially crafted network request to the vulnerable service and a user interacting with the service's client application on the host. In order to execute arbitrary code with Microsoft Windows user permissions, an attacker must be able to plant the code in advance on the host by other means. The vulnerability has limited impact to confidentiality and integrity of the affected system	COMMAND INJECTION EAVESDROPPING
- - - - - - - - - - - - Siemens SIMATIC WinCC (TIA Portal) 13.0 Siemens SIMATIC WinCC 7.4 Service Pack 1 Update 3 ————— Siemens SIMATIC WinCC Runtime Professional 13 Special Pack 1	CVE-2019-10916	https://nvd.nist.gov/vuln/detail/CVE-2019-10916	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I: H/A:H **8,8 HIGH**	HIGH;HIGH;HIGH	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	An attacker with access to the project file could run arbitrary system commands with the privileges of the local database server, and therefore it takes a bit hit in CIA	COMMAND INJECTION FALSE DATA INJECTION
- - - - - - - - - - - - Siemens SIMATIC WinCC (TIA Portal) 13.0 Siemens SIMATIC WinCC 7.4 Service Pack 1 Update 3 ————— Siemens SIMATIC WinCC Runtime Professional 13 Special Pack 1	CVE-2019-10917	https://nvd.nist.gov/vuln/detail/CVE-2019-10917	AV:L/AC:L/PR:L/UI:N/S:U/C:N/I: N/A:H **5,5 MEDIUM**	none;none;HIGH	Improper Handling of Exceptional Conditions	An attacker with local access to the project file could cause a Denial-of-Service condition on the affected product while the project file is loaded. Successful exploitation requires access to the project file	DENIAL OF SERVICE

Siemens SIMATIC WinCC (TIA Portal) 13.0 Siemens SIMATIC WinCC 7.4 Service Pack 1 Update 3 —————— Siemens SIMATIC WinCC Runtime Professional 13 Special Pack 1	CVE-2019-10918	https://nvd.nist.gov/vuln/detail/CVE-2019-10918	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I: H/A:H **8,8 HIGH**	HIGH;HIGH;HIGH	Exposed Dangerous Method or Function	An authenticatd attacker with network access to the DCOM interface could execute arbitrary commands with SYSTEM privileges.	COMMAND INJECTION
Siemens SIMATIC WinCC 7.4 Service Pack 1 Update 3	CVE-2019-10922	https://nvd.nist.gov/vuln/detail/CVE-2019-10922	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I: H/A:H **9,8 CRITICAL**	HIGH;HIGH;HIGH	Missing Authentication for Critical Function	An attacker with network access to affected installations, which are configured without "Encrypted Communication", can execute arbitrary code. The security vulnerability could be exploited by an unauthenticated attacker with network access to the affected installation.	COMMAND INJECTION
Siemens SINAMICS G120	CVE-2019-10923	https://nvd.nist.gov/vuln/detail/CVE-2019-10923	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I: N/A:H **7,5 HIGH**	none;none;HIGH	Uncontrolled Resource Consumption	An attacker with network access to an affected product may cause a denial of service condition by breaking the real-time synchronization (IRT) of the affected installation	DENIAL OF SERVICE
Siemens SIMATIC WinCC 7.4 Service Pack 1 Update 3	CVE-2019-10929	https://nvd.nist.gov/vuln/detail/CVE-2019-10929	AV:N/AC:H/PR:N/UI:N/S:U/C:N/I: H/A:N **5,9 MEDIUM**	none;HIGH;none	Use of a Broken or Risky Cryptographic Algorithm	Affected devices contain a message protection bypass vulnerability due to certain properties in the calculation used for integrity protection. This could allow an attacker in a Man-in-the- Middle position to modify network traffic sent on port 102/tcp to the affected devices.	FALSE DATA INJECTION EAVESDROPPING
SIPROTEC	CVE-2019-10930	https://nvd.nist.gov/vuln/detail/CVE-2019-10930	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I: H/A:N **7,5 HIGH**	none;HIGH;none	Unrestricted Upload of File with Dangerous Type	A remote attacker could use specially crafted packets sent to port 443/TCP to upload, download or delete files in certain parts of the file system.	FALSE DATA INJECTION EAVESDROPPING
SIPROTEC	CVE-2019-10931	https://nvd.nist.gov/vuln/detail/CVE-2019-10931	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I: N/A:H **7,5 HIGH**	none;none;HIGH	Uncaught Exception	Specially crafted packets sent to port 443/TCP could cause a Denial of Service condition.	DENIAL OF SERVICE

Siemens SIMATIC S7-1500 CPU ————— Siemens SINAMICS G120	CVE-2019-10936	https://nvd.nist.gov/vuln/detail/CVE-2019-10936	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I: N/A:H **7,5 HIGH**	none;none;HIGH	Uncontrolled Resource Consumption - Affected devices improperly handle large amounts of specially crafted UDP packets.	could allow an unauthenticated remote attacker to trigger a denial of service condition.	DENIAL OF SERVICE
SIPROTEC	CVE-2019-10938	https://nvd.nist.gov/vuln/detail/CVE-2019-10938	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I: H/A:H **9,8 CRITICAL**	HIGH;HIGH;HIGH	Improper Access Control	An unauthenticated attacker with network access to the device could potentially insert arbitrary code which is executed before firmware verification in the device	COMMAND INJECTION
Siemens SIMATIC S7-1500 Software Controller	CVE-2019-10943	https://nvd.nist.gov/vuln/detail/CVE-2019-10943	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I: H/A:N **7,5 HIGH**	none;HIGH;none	Insufficient Verification of Data Authenticity - The vulnerability could impact the perceived integrity of the user program stored on the CPU	An attacker with network access to port 102/tcp could potentially modify the user program on the PLC in a way that the running code is different from the source code which is stored on the device	COMMAND INJECTION
Siemens S7-1200 CPU 1211C; 1212C 1212f 1214C 1214fc 1215C 1215fc 1217c	CVE-2019-13940	https://nvd.nist.gov/vuln/detail/CVE-2019-13940	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I: N/A:H **7,5 HIGH**	none;none;HIGH	Uncontrolled Resource Consumption	an attacker could send specially crafted HTTP requests to ports 80/tcp and 443/tcp and lead to a DoS of the web server	DENIAL OF SERVICE
Esri ArcGIS Enterprise Esri ArcGIS Enterprise 10.6.1	CVE-2019-16193	https://nvd.nist.gov/vuln/detail/CVE-2019-16193	AV:N/AC:L/PR:L/UI:R/S:C/C:L/I: L/A:N **5,4 MEDIUM**	LOW;LOW;none	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	can be used to trigger a Cross Frame Scripting (XFS) attack through the EDIT MY PROFILE feature.	COMMAND INJECTION
SIPROTEC	CVE-2019-19279	https://nvd.nist.gov/vuln/detail/CVE-2019-19279	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I: N/A:H **7,5 HIGH**	none;none;HIGH	Improper Input Validation	Specially crafted packets sent to port 50000/UDP of the EN100 Ethernet communication modules could cause a Denial-of-Service of the affected device. A manual reboot is required to recover the service of the device.	DENIAL OF SERVICE
Siemens SIMATIC S7-1500 Software Controller	CVE-2019-6568	https://nvd.nist.gov/vuln/detail/CVE-2019-6568	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I: N/A:H **7,5 HIGH**	none;none;HIGH	Out-of-bounds Read	Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise availability of the device	DENIAL OF SERVICE

Siemens SIMATIC WinCC (TIA Portal) 13.0	CVE-2019-6572	https://nvd.nist.gov/vuln/detail/CVE-2019-6572	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I: H/A:N **9,1 CRITICAL**	HIGH;HIGH;none	Use of Hard-coded Credentials - The affected device offered SNMP read and write capacities with a publicly know hardcoded community string	An attacker could use the vulnerability to compromise confidentiality and integrity of the affected system.	FALSE DATA INJECTION EAVESDROPPING
Siemens SIMATIC S7-1500 Software Controller	CVE-2019-6575	https://nvd.nist.gov/vuln/detail/CVE-2019-6575	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I: N/A:H **7,5 HIGH**	none;none;HIGH	Improper Handling of Exceptional Conditions - Specially crafted network packets sent to affected devices on port 4840/tcp	Could allow an unauthenticated remote attacker to cause a denial of service condition of the OPC communication or crash the device.	DENIAL OF SERVICE
Siemens SIMATIC WinCC (TIA Portal) 13.0	CVE-2019-6576	https://nvd.nist.gov/vuln/detail/CVE-2019-6576	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I: N/A:N **7,5 HIGH**	HIGH;none;none	Cryptographic Issues	An attacker with network access to affected devices could potentially obtain a TLS session key. If the attacker is able to observe TLS traffic between a legitimate user and the device, then the attacker could decrypt the TLS traffic. The security vulnerability could be exploited by an attacker who has network access to the web interface of the device and who is able to observe TLS traffic between legitimate users and the web interface of the affected device. The vulnerability could impact the confidentiality of the communication between the affected device and a legitimate user.	EAVESDROPPING
Siemens SIMATIC WinCC (TIA Portal) 13.0	CVE-2019-6577	https://nvd.nist.gov/vuln/detail/CVE-2019-6577	AV:N/AC:L/PR:L/UI:R/S:C/C:L/I: L/A:N **5,4 MEDIUM**	LOW;LOW;none	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	The integrated web server could allow Cross-Site Scripting (XSS) attacks if an attacker is able to modify particular parts of the device configuration via SNMP. The security vulnerability could be exploited by an attacker with network access to the affected system. Successful exploitation requires system privileges and user interaction. An attacker could use the vulnerability to compromise confidentiality and the integrity of the affected system.	FALSE DATA INJECTION EAVESDROPPING

Siemens SICAM MMU Siemens SICAM SGU Siemens SICAM T Siemens SICAM SGU Firmware	CVE-2020-10037	https://nvd.nist.gov/vuln/detail/CVE-2020-10037	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I: N/A:N **7,5 HIGH**	HIGH;none;none	Out-of-bounds Read	By performing a flooding attack against the web server, an attacker might be able to gain read access to the device's memory, possibly revealing confidential information	EAVESDROPPING
Siemens SICAM MMU Siemens SICAM SGU Siemens SICAM T Siemens SICAM SGU Firmware	CVE-2020-10038	https://nvd.nist.gov/vuln/detail/CVE-2020-10038	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I: H/A:H **9,8 CRITICAL**	HIGH;HIGH;HIGH	Missing Authentication for Critical Function	An attacker with access to the device's web server might be able to execute administrative commands without authentication.	COMMAND INJECTION
Siemens SICAM MMU Siemens SICAM SGU Siemens SICAM T Siemens SICAM SGU Firmware	CVE-2020-10039	https://nvd.nist.gov/vuln/detail/CVE-2020-10039	AV:N/AC:H/PR:N/UI:N/S:U/C:H/I: H/A:H **8,1 HIGH**	HIGH;HIGH;HIGH	Missing Encryption of Sensitive Data	An attacker in a privileged network position between a legitimate user and the web server might be able to conduct a Man-in-the-middle attack and gain read and write access to the transmitted data	FALSE DATA INJECTION EAVESDROPPING
Siemens SICAM MMU Siemens SICAM SGU Siemens SICAM T Siemens SICAM SGU Firmware	CVE-2020-10040	https://nvd.nist.gov/vuln/detail/CVE-2020-10040	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I: N/A:N **5,5 MEDIUM**	HIGH;none;none	Use of Password Hash With Insufficient Computational Effort	An attacker with local access to the device might be able to retrieve some passwords in clear text.	EAVESDROPPING
Siemens SICAM MMU Siemens SICAM SGU Siemens SICAM T Siemens SICAM SGU Firmware	CVE-2020-10041	https://nvd.nist.gov/vuln/detail/CVE-2020-10041	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I: L/A:N **6,1 MEDIUM**	LOW;LOW;none	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	An attacker might be able to take over a session of a legitimate user.	LATERAL MOVEMENT / PRIVILEGE ESCALATION
Siemens SICAM MMU Siemens SICAM SGU Siemens SICAM T Siemens SICAM SGU Firmware	CVE-2020-10042	https://nvd.nist.gov/vuln/detail/CVE-2020-10042	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I: H/A:H **9,8 CRITICAL**	HIGH;HIGH;HIGH	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	might enable an attacker with access to the web application to execute arbitrary code over the network.	COMMAND INJECTION DENIAL OF SERVICE
Siemens SICAM MMU Siemens SICAM SGU Siemens SICAM T Siemens SICAM SGU Firmware	CVE-2020-10043	https://nvd.nist.gov/vuln/detail/CVE-2020-10043	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I: L/A:N **6,1 MEDIUM**	LOW;LOW;none	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	could allow Cross-Site Scripting (XSS) attacks if unsuspecting users are tricked into accessing a malicious link.	OTHER
Siemens SICAM MMU Siemens SICAM SGU Siemens SICAM T Siemens SICAM SGU Firmware	CVE-2020-10044	https://nvd.nist.gov/vuln/detail/CVE-2020-10044	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I: H/A:N **7,5 HIGH**	none;HIGH;none	Missing Authentication for Critical Function	An attacker with access to the network could be able to install specially crafted firmware to the device.	FALSE DATA INJECTION PERSISTENCE
Siemens SICAM MMU Siemens SICAM SGU Siemens SICAM T Siemens SICAM SGU Firmware	CVE-2020-10045	https://nvd.nist.gov/vuln/detail/CVE-2020-10045	AV:N/AC:L/PR:N/UI:R/S:U/C:H/I: H/A:H **8,8 HIGH**	HIGH;HIGH;HIGH	Authentication Bypass by Capture-replay	An error in the challenge- response procedure could allow an attacker to replay authentication traffic and gain access to protected areas of the web application.	ACCESS

Siemens SIMATIC WinCC 7.4 Service Pack 1 Update 3	CVE-2020-10048	https://nvd.nist.gov/vuln/detail/CVE-2020-10048	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I: N/A:N **5,5 MEDIUM**	HIGH;none;none	Improper Authentication - insecure password verification process	An attacker could bypass the password protection set on protected files, thus being granted access to the protected content, circumventing authentication.	EAVESDROPPING
Siemens SICAM A8000	CVE-2020-15781	https://nvd.nist.gov/vuln/detail/CVE-2020-15781	AV:N/AC:L/PR:N/UI:R/S:C/C:H/I: H/A:H **9,6 CRITICAL**	HIGH;HIGH;HIGH	**XSS -** The login screen does not sufficiently sanitize input, which enables an attacker to generate specially crafted log messages. If an unsuspecting victim views the log messages via the web browser, these log messages might be interpreted and executed as code by the web application.	This Cross-Site-Scripting (XSS) vulnerability might compromize the confidentiality, integrity and availability of the web application.	OTHER
Siemens SIMATIC ET 200SP Open Controller	CVE-2020-15796	https://nvd.nist.gov/vuln/detail/CVE-2020-15796	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I: N/A:H **7,5 HIGH**	none;none;HIGH	Uncaught Exception	could allow a remote attacker to trigger a denial-of-service condition by sending a specially crafted HTTP request	DENIAL OF SERVICE
Siemens SIMATIC ET 200SP Open Controller	CVE-2020-24513	https://nvd.nist.gov/vuln/detail/CVE-2020-24513	AV:L/AC:L/PR:L/UI:N/S:C/C:H/I: N/A:N **6,6 MEDIUM**	HIGH;none;none	Domain-bypass transient execution vulnerability	could allow an attacker to disclose confidential information if they are connected to the local network	EAVESDROPPING
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 on X64 Esri ArcGIS Server 10.6.1 on X64 Esri ArcGIS Server 10.7.1 on X64	CVE-2020-35712	https://nvd.nist.gov/vuln/detail/CVE-2020-35712	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I: H/A:H **9,8 CRITICAL**	HIGH;HIGH;HIGH	SSRF	an attacker could retrieve senstivie information from the server	EAVESDROPPING
Siemens SIMATIC WinCC Runtime Professional 13 Special Pack 1 ———————— Siemens SIMATIC S7-1500 Software Controller	CVE-2020-7580	https://nvd.nist.gov/vuln/detail/CVE-2020-7580	AV:L/AC:L/PR:H/UI:N/S:U/C:H/I: H/A:H **6,7 MEDIUM**	HIGH;HIGH;HIGH	A common component used by the affected applications regularly calls a helper binary with SYSTEM privileges while the call path is not quoted.	This could allow a local attacker to execute arbitrary code with SYTEM privileges.	COMMAND INJECTION

ABB RER620 - ABB RER620 FIRMWARE ABB SMU615 - ABB SMU615 FIRMWARE	CVE-2021-22283	https://nvd.nist.gov/vuln/detail/CVE-2021-22283	AV:L/AC:L/PR:N/UI:N/S:U/C:N/I: N/A:H **6,2 MEDIUM —> ABB** AV:L/AC:L/PR:L/UI:N/S:U/C:N/I: N/A:H **5,5 MEDIUM** —> NIST	none;none;HIGH	Improper Initialization	An attacker could exploit the vulnerabilities by using a specially crafted MMS client, which opens multiple files with file open requests without never closing the files. This would cause the relay to go to an internal fault state.	DENIAL OF SERVICE
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	CVE-2021-29093	https://nvd.nist.gov/vuln/detail/CVE-2021-29093	AV:N/AC:L/PR:H/UI:R/S:U/C:H/I: H/A:H **6,8 MEDIUM**	HIGH;HIGH;HIGH	use-after-free vulnerability when parsing a specially crafted file	allows an authenticated attacker with specialized permissions to achieve arbitrary code execution in the context of the service account	COMMAND INJECTION
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	CVE-2021-29094	https://nvd.nist.gov/vuln/detail/CVE-2021-29094	AV:N/AC:L/PR:H/UI:R/S:U/C:H/I: H/A:H **6,8 MEDIUM**	HIGH;HIGH;HIGH	Multiple buffer overflow vulnerabilities when parsing a specially crafted file	allows an authenticated attacker with specialized permissions to achieve arbitrary code execution in the context of the service account	COMMAND INJECTION
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	CVE-2021-29095	https://nvd.nist.gov/vuln/detail/CVE-2021-29095	AV:N/AC:L/PR:H/UI:R/S:U/C:H/I: H/A:H **6,8 MEDIUM**	HIGH;HIGH;HIGH	Multiple uninitialized pointer vulnerabilities when parsing a specially crafted file	allows an authenticated attacker with specialized permissions to achieve arbitrary code execution in the context of the service account	COMMAND INJECTION
ESRI ArcGIS Desktop ESRI ArcGIS Desktop 10.8.1 Esri ArcGIS Engine 10.3 - 8; 10.8.1 —————————— Esri ArcGIS Pro 2.6; 2.6.5; 2.7;	CVE-2021-29096	https://nvd.nist.gov/vuln/detail/CVE-2021-29096	AV:L/AC:L/PR:N/UI:R/S:U/C:H/I: H/A:H **7,8 HIGH**	HIGH;HIGH;HIGH	use-after-free vulnerability when parsing a specially crafted file	allow an **unauthenticated** attacker to achieve arbitrary code execution in the context of the current user.	COMMAND INJECTION
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 Desktop ESRI ArcGIS Desktop 10.8.1 —————————— Esri ArcGIS Pro 2.6; 2.6.5; 2.7;	CVE-2021-29097	https://nvd.nist.gov/vuln/detail/CVE-2021-29097	AV:L/AC:L/PR:N/UI:R/S:U/C:H/I: H/A:H **7,8 HIGH**	HIGH;HIGH;HIGH	Multiple buffer overflow vulnerabilities when parsing a specially crafted file	allow an **unauthenticated** attacker to achieve arbitrary code execution in the context of the current user.	COMMAND INJECTION

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 Desktop ESRI ArcGIS Desktop 10.8.1 —————————— Esri ArcGIS Pro 2.6; 2.6.5; 2.7;	CVE-2021-29098	https://nvd.nist.gov/vuln/detail/CVE-2021-29098	AV:L/AC:L/PR:N/UI:R/S:U/C:H/I: H/A:H **7,8 HIGH**	HIGH;HIGH;HIGH	Multiple uninitialized pointer vulnerabilities when parsing a specially crafted file	allow an **unauthenticated** attacker to achieve arbitrary code execution in the context of the current user.	COMMAND INJECTION
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 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	CVE-2021-29099	https://nvd.nist.gov/vuln/detail/CVE-2021-29099	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I: N/A:N **5,3 MEDIUM**	LOW;none;none	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Specially crafted web requests can expose information	EAVESDROPPING

Esri ArcGIS Earth 1.7.0; 1.8.0;
1.9.0;
1.10.0;
1.10.1;
1.11.0;
	CVE-2021-29100	https://nvd.nist.gov/vuln/detail/CVE-2021-29100	AV:L/AC:L/PR:N/UI:R/S:U/C:H/I: H/A:H **7,8 HIGH**	HIGH;HIGH;HIGH	A path traversal vulnerability	An attacker could exploit this vulnerability to gain arbitrary code execution under security context of the user running ArcGIS Earth by inducing the user to upload a crafted file to an affected system	COMMAND INJECTION
							FALSE DATA INJECTION

ArcGIS GeoEvent Server ArcGIS GeoEvent Server 10.8.1	CVE-2021-29101	https://nvd.nist.gov/vuln/detail/CVE-2021-29101	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I: N/A:N **7,5 HIGH**	HIGH;none;none	has a read-only directory path traversal vulnerability	could allow an unauthenticated, remote attacker to perform directory traversal attacks and read arbitrary files on the system	EAVESDROPPING
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	CVE-2021-29102	https://nvd.nist.gov/vuln/detail/CVE-2021-29102	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I: H/A:N **9,1 CRITICAL**	HIGH;HIGH;none	Server-Side Request Forgery (SSRF)	may allow a **remote, unauthenticated** attacker to forge GET requests to arbitrary URLs from the system, potentially leading to network enumeration or facilitating other attacks	EAVESDROPPING

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	CVE-2021-29103	https://nvd.nist.gov/vuln/detail/CVE-2021-29103	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I: L/A:N **6,1 MEDIUM**	LOW;LOW;none	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') - reflected Cross Site Scripting (XXS)	a remote attacker able to convince a user to click on a crafted link which could potentially execute arbitrary JavaScript code in the user's browser. This way an experience attacker could get to infect different systems of the grid	OTHER
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	CVE-2021-29104	https://nvd.nist.gov/vuln/detail/CVE-2021-29104	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I: L/A:N **6,1 MEDIUM**	LOW;LOW;none	stored Cross Site Scripting (XXS)	allow a **remote unauthenticated** attacker to pass and store malicious strings in the application	FALSE DATA INJECTION
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	CVE-2021-29105	https://nvd.nist.gov/vuln/detail/CVE-2021-29105	AV:N/AC:L/PR:L/UI:R/S:C/C:L/I: L/A:N **5.4 MEDIUM**	LOW;LOW;none	stored Cross Site Scripting (XSS)	may allow a **remote authenticated** attacker to pass and store malicious strings in the ArcGIS Services Directory	FALSE DATA INJECTION
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	CVE-2021-29106	https://nvd.nist.gov/vuln/detail/CVE-2021-29106	AV:N/AC:H/PR:N/UI:R/S:C/C:L/I: L/A:N **4,7 MEDIUM** —> ESRI AV:N/AC:L/PR:N/UI:R/S:C/C:L/I: L/A:N **6,1 MEDIUM** —> NIST	LOW;LOW;none	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') - reflected Cross Site Scripting (XXS)	a remote attacker able to convince a user to click on a crafted link which could potentially execute arbitrary JavaScript code in the user's browser. This way an experience attacker could get to infect different systems of the grid	OTHER
Esri ArcGIS Server 10.6.1 on X64	CVE-2021-29107	https://nvd.nist.gov/vuln/detail/CVE-2021-29107	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I: L/A:N **6,1 MEDIUM**	LOW;LOW;none	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	may allow a remote unauthenticated attacker to pass and store malicious strings in the ArcGIS Server Manager application.	FALSE DATA INJECTION
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	CVE-2021-29108	https://nvd.nist.gov/vuln/detail/CVE-2021-29108	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I: H/A:H **8,8 HIGH**	HIGH;HIGH;HIGH	privilege escalation vulnerability	may allow a remote, authenticated attacker who is able to intercept and modify a SAML assertion to impersonate another account (XML Signature Wrapping Attack)	LATERAL MOVEMENT / PRIVILEGE ESCALATION

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	CVE-2021-29109	https://nvd.nist.gov/vuln/detail/CVE-2021-29109	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I: L/A:N **6,1 MEDIUM**	LOW;LOW;none	reflected XSS	may allow a remote attacker able to convince a user to click on a crafted link which could potentially execute arbitrary JavaScript code in the user's browser.	OTHER
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	CVE-2021-29110	https://nvd.nist.gov/vuln/detail/CVE-2021-29110	AV:N/AC:L/PR:L/UI:R/S:C/C:L/I: L/A:N **5,4 MEDIUM**	LOW;LOW;none	Stored cross-site scripting (XSS)	may allow a remote unauthenticated attacker to pass and store malicious strings in the home application. This could later on lead to other attacks.	FALSE DATA INJECTION
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	CVE-2021-29113	https://nvd.nist.gov/vuln/detail/CVE-2021-29113	AV:N/AC:L/PR:N/UI:R/S:C/C:N/I: L/A:N **4,7 MEDIUM**	none;LOW;none	remote file inclusion vulnerability	may allow a **remote, unauthenticated** attacker to inject attacker supplied html into a page. This way an attacker could do a XSS attack, phishing, distribute malware and so on.	OTHER
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	CVE-2021-29114	https://nvd.nist.gov/vuln/detail/CVE-2021-29114	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I: L/A:L **7,3 HIGH** —> ESRI AV:N/AC:L/PR:N/UI:N/S:U/C:H/I: H/A:H **9,8 CRITICAL** —> NIST	LOW;LOW;LOW	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	allows a **remote, unauthenticated** attacker to impact the confidentiality, integrity and availability of targeted services via specifically crafted queries	FALSE DATA INJECTION EAVESDROPPING DENIAL OF SERVICE

Esri ArcGIS Enterprise Esri ArcGIS Enterprise 10.6.1 Esri ArcGIS Enterprise 10.9	CVE-2021-29115	https://nvd.nist.gov/vuln/detail/CVE-2021-29115	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I: N/A:N **5,3 MEDIUM**	LOW;none;none	information disclosure vulnerability	allows a remote attacker to view hidden field names in feature layers. This issue may reveal field names, but not not disclose features	EAVESDROPPING
Esri ArcGIS Server 10.8.1 Esri ArcGIS Server 10.9.0 Esri ArcGIS Server 10.8.1 on X64 Esri ArcGIS Server 10.9.0 on X64	CVE-2021-29116	https://nvd.nist.gov/vuln/detail/CVE-2021-29116	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I: L/A:N **6,1 MEDIUM**	LOW;LOW;none	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	may allow a remote, unauthenticated attacker to pass and store malicious strings via crafted queries which when accessed could potentially execute arbitrary JavaScript code in the user's browser.	COMMAND INJECTION
Esri ArcGIS Enterprise Esri ArcGIS Enterprise 10.6.1	CVE-2021-3012	https://nvd.nist.gov/vuln/detail/CVE-2021-3012	AV:N/AC:L/PR:L/UI:R/S:C/C:L/I: L/A:N **5.4 MEDIUM**	LOW;LOW;none	**cross-site scripting (XSS)**	allows remote **authenticated** users to inject arbitrary JavaScript code via a malicious HTML attribute such as onerror (in the URL field of the Parameters tab)	COMMAND INJECTION
SIPROTEC	CVE-2021-33719	https://nvd.nist.gov/vuln/detail/CVE-2021-33719	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I: H/A:H **9,8 CRITICAL**	HIGH;HIGH;HIGH	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	Specially crafted packets sent to port 4443/tcp could cause a Denial-of-Service condition **or potential remote code execution.**	COMMAND INJECTION
SIPROTEC	CVE-2021-33720	https://nvd.nist.gov/vuln/detail/CVE-2021-33720	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I: N/A:H **7,5 HIGH**	none;none;HIGH	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	Specially crafted packets sent to port 4443/tcp could cause a Denial-of-Service condition.	DENIAL OF SERVICE
Siemens SIMATIC S7-1500 Software Controller	CVE-2021-37185	https://nvd.nist.gov/vuln/detail/CVE-2021-37185	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I: N/A:H **7,5 HIGH**	none;none;HIGH	Operation on a Resource after Expiration or Release	An unauthenticated attacker could cause a denial-of-service condition in a PLC when sending specially prepared packets over port 102/tcp. A restart of the affected device is needed to restore normal operations.	DENIAL OF SERVICE
Siemens SIMATIC S7-1500 Software Controller	CVE-2021-37204	https://nvd.nist.gov/vuln/detail/CVE-2021-37204	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I: N/A:H **7,5 HIGH**	none;none;HIGH	Operation on a Resource after Expiration or Release	An unauthenticated attacker could cause a denial-of-service condition in a PLC when sending specially prepared packet over port 102/tcp. A restart of the affected device is needed to restore normal operations.	DENIAL OF SERVICE

Siemens SIMATIC S7-1500 Software Controller	CVE-2021-37205	https://nvd.nist.gov/vuln/detail/CVE-2021-37205	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I: N/A:H **7,5 HIGH**	none;none;HIGH	Missing Release of Memory after Effective Lifetime	An unauthenticated attacker could cause a denial-of-service condition in a PLC when sending specially prepared packets over port 102/tcp. A restart of the affected device is needed to restore normal operations.	DENIAL OF SERVICE
SIPROTEC	CVE-2021-37206	https://nvd.nist.gov/vuln/detail/CVE-2021-37206	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I: N/A:H **7,5 HIGH**	none;none;HIGH	Improper Input Validation - Received webpackets are not properly processed	An unauthenticated remote attacker with access to any of the Ethernet interfaces could send specially crafted packets to force a restart of the target device.	DENIAL OF SERVICE
Siemens SIMATIC WinCC 7.4 Service Pack 1 Update 3	CVE-2021-40358	https://nvd.nist.gov/vuln/detail/CVE-2021-40358	AV:N/AC:L/PR:L/UI:N/S:C/C:H/I: H/A:H **9,9 CRITICAL —> SIEMENS** AV:N/AC:L/PR:N/UI:N/S:U/C:H/I: H/A:H **9,8 CRITICAL** —> NIST	HIGH;HIGH;HIGH	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') - Legitimate file operations on the web server of the affected systems do not properly neutralize 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, write or delete unexpected critical files.	FALSE DATA INJECTION EAVESDROPPING DENIAL OF SERVICE
Siemens SIMATIC WinCC 7.4 Service Pack 1 Update 3	CVE-2021-40359	https://nvd.nist.gov/vuln/detail/CVE-2021-40359	AV:N/AC:L/PR:L/UI:N/S:C/C:H/I: N/A:N **7,7 HIGH —> SIEMENS** AV:N/AC:L/PR:N/UI:N/S:U/C:H/I: N/A:N **7,5 HIGH** —> NIST	HIGH;none;none	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') - When downloading files, the affected systems do not properly neutralize 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.	EAVESDROPPING
Siemens SIMATIC WinCC 7.4 Service Pack 1 Update 3	CVE-2021-40364	https://nvd.nist.gov/vuln/detail/CVE-2021-40364	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I: N/A:N **5,5 MEDIUM**	HIGH;none;none	Insertion of Sensitive Information into Log File - The affected systems store sensitive information in log files	An attacker with access to the log files could publicly expose the information or reuse it to develop further attacks on the system.	EAVESDROPPING

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	CVE-2021-40365	https://nvd.nist.gov/vuln/detail/CVE-2021-40365	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I: N/A:H **7,5 HIGH**	none;none;HIGH	Improper Input Validation - . Affected devices don't process correctly certain special crafted packets sent to port 102/tcp	could allow an attacker to cause a denial of service in the device	DENIAL OF SERVICE
SIPROTEC	CVE-2021-41769	https://nvd.nist.gov/vuln/detail/CVE-2021-41769	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I: N/A:N **7,5 HIGH**	HIGH;none;none	Improper Input Validation	An improper input validation vulnerability in the web server could allow an unauthenticated user to access device information.	EAVESDROPPING
Siemens SIMATIC S7-1500 CPU	CVE-2021-42029	https://nvd.nist.gov/vuln/detail/CVE-2021-42029	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I: H/A:H **7,8 HIGH**	HIGH;HIGH;HIGH	Improper Access Control	An attacker could achieve privilege escalation on the web server of certain devices	LATERAL MOVEMENT / PRIVILEGE ESCALATION
Siemens (SICAM Q100) 7KG9501-0AA01-0AA1 —————— Siemens (SICAM Q100) 7KG9501-0AA31-2AA1	CVE-2021-44165	https://nvd.nist.gov/vuln/detail/CVE-2021-44165	AV:N/AC:L/PR:H/UI:N/S:U/C:H/I: H/A:H **7,2 HIGH**	HIGH;HIGH;HIGH	Stack-based Buffer Overflow	could allow a remote attacker with engineer or admin priviliges to potentially perform remote code execution.	COMMAND INJECTION
Siemens EnergyIP 8.5 Siemens EnergyIP 8.6 Siemens EnergyIP 8.7 Siemens EnergyIP 9.0 ———————————— Siemens SIGUARD DSA 4.2 Siemens SIGUARD DSA 4.3 Siemens SIGUARD DSA 4.4	CVE-2021-44228	https://nvd.nist.gov/vuln/detail/CVE-2021-44228	AV:N/AC:L/PR:N/UI:N/S:C/C:H/I: H/A:H **10,0 CRITICAL**	HIGH;HIGH;HIGH	log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints	An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled.	COMMAND INJECTION

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	CVE-2021-44693	https://nvd.nist.gov/vuln/detail/CVE-2021-44693	AV:N/AC:L/PR:N/UI:N/S: U/C:N/I: N/A:H **7,5 HIGH**	none;none;HIGH	Improper Input Validation - . Affected devices don't process correctly certain special crafted packets sent to port 102/tcp	could allow an attacker to cause a denial of service in the device	DENIAL OF SERVICE
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	CVE-2021-44694	https://nvd.nist.gov/vuln/detail/CVE-2021-44694	AV:N/AC:L/PR:N/UI:N/S: U/C:N/I: N/A:H **7,5 HIGH**	none;none;HIGH	Improper Input Validation - . Affected devices don't process correctly certain special crafted packets sent to port 102/tcp	could allow an attacker to cause a denial of service in the device	DENIAL OF SERVICE

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	CVE-2021-44695	https://nvd.nist.gov/vuln/detail/CVE-2021-44695	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I: N/A:H **7,5 HIGH**	none;none;HIGH	Improper Input Validation - . Affected devices don't process correctly certain special crafted packets sent to port 102/tcp	could allow an attacker to cause a denial of service in the device	DENIAL OF SERVICE
Siemens EnergyIP 8.5 Siemens EnergyIP 8.6 ~~Siemens EnergyIP 8.7 -~~ Siemens EnergyIP 9.0 Siemens SIGUARD DSA 4.2 Siemens SIGUARD DSA 4.3 Siemens SIGUARD DSA 4.4	CVE-2021-45046	https://nvd.nist.gov/vuln/detail/CVE-2021-45046	AV:N/AC:H/PR:N/UI:N/S:C/C:H/I: H/A:H **9,0 CRITICAL**	HIGH;HIGH;HIGH	Improper Neutralization of Special Elements used in an Expression Language Statement		FALSE DATA INJECTION
Siemens SICAM Toolbox II	CVE-2021-45106	https://nvd.nist.gov/vuln/detail/CVE-2021-45106	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I: N/A:N **6,5 MEDIUM**	HIGH;none;none	Use of Hard-coded Credentials - Affected applications use a circumventable access control within a database service	This could allow an attacker to access the database.	EAVESDROPPING
Siemens SICAM PQ ANALYZER	CVE-2021-45460	https://nvd.nist.gov/vuln/detail/CVE-2021-45460	AV:N/AC:L/PR:L/UI:N/S:U/C:N/I: H/A:H **8,1 HIGH**	none;HIGH;HIGH	Unquoted Search Path or Element - A service is started by an unquoted registry entry	As there are spaces in this path, attackers with write privilege to those directories might be able to plant executables that will run in place of the legitimate process. Attackers might achieve persistence on the system ("backdoors") or cause a denial of service	FALSE DATA INJECTION DENIAL OF SERVICE PERSISTENCE
Siemens SIMATIC WinCC Runtime Professional 13 Special Pack 1	CVE-2022-24287	https://nvd.nist.gov/vuln/detail/CVE-2022-24287	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I: H/A:H **7,8 HIGH**	HIGH;HIGH;HIGH	Insecure Default Initialization of Resource - a missing printer configuration on the host could allow an authenticated attacker to escape the WinCC Kiosk Mode.	This could allow an attacker to view sensitive information, run tasks outside the intended scope and therefore have an impact in the CIA	EAVESDROPPING

Siemens SIMATIC WinCC Runtime Professional 13 Special Pack 1 ———— Siemens SIMATIC WinCC 7.4 Service Pack 1 Update 3	CVE-2022-24287	https://nvd.nist.gov/vuln/detail/CVE-2022-24287	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I: H/A:H **7,8 HIGH**	HIGH;HIGH;HIGH	Insecure Default Initialization of Resource - a missing printer configuration on the host could allow an authenticated attacker to escape the WinCC Kiosk Mode.	This could allow an attacker to view sensitive information, run tasks outside the intended scope and therefore have an impact in the CIA	EAVESDROPPING
Siemens SIMATIC S7-1500 CPU	CVE-2022-25622	https://nvd.nist.gov/vuln/detail/CVE-2022-25622	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I: N/A:L **5,3 MEDIUM—> SIEMENS** AV:N/AC:L/PR:N/UI:N/S:U/C:N/I: N/A:H **7,5 HIGH** —> NIST	none;none;LOW	Uncontrolled Resource Consumption - The PROFINET (PNIO) stack, when integrated with the Interniche IP stack, improperly handles internal resources for TCP segments where the minimum TCP-Header length is less than defined	could allow an attacker to create a denial of service condition for TCP services on affected devices by sending specially crafted TCP segments.	DENIAL OF SERVICE
SICAM P850 ———— SICAM P855	CVE-2022-29872	https://nvd.nist.gov/vuln/detail/CVE-2022-29872	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I: H/A:H **8,8 HIGH**	HIGH;HIGH;HIGH	Improper Input Validation - Affected devices do not properly validate parameters of POST requests	This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device.	COMMAND INJECTION DENIAL OF SERVICE
SICAM P850 ———— SICAM P855	CVE-2022-29873	https://nvd.nist.gov/vuln/detail/CVE-2022-29873	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I: H/A:H **9,8 CRITICAL**	HIGH;HIGH;HIGH	Improper Neutralization of Parameter/Argument Delimiters - Affected devices do not properly validate parameters of certain GET and POST requests.	Could allow an unauthenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device.	COMMAND INJECTION DENIAL OF SERVICE
SICAM P850 ———— SICAM P855	CVE-2022-29874	https://nvd.nist.gov/vuln/detail/CVE-2022-29874	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I: N/A:N **7,5 HIGH**	HIGH;none;none	Cleartext Transmission of Sensitive Information - Affected devices do not encrypt web traffic with clients but communicate in cleartext via HTTP	This could allow an unauthenticated attacker to capture the traffic and interfere with the functionality of the device.	EAVESDROPPING
SICAM P850 ———— SICAM P855	CVE-2022-29876	https://nvd.nist.gov/vuln/detail/CVE-2022-29876	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I: L/A:N **6,1 MEDIUM**	LOW;none;none	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') - Affected devices do not properly handle the input of a GET request parameter.	The provided argument is directly reflected in the web server response. This could allow an unauthenticated attacker to perform reflected XSS attacks.	OTHER
SICAM P850 ———— SICAM P855	CVE-2022-29877	https://nvd.nist.gov/vuln/detail/CVE-2022-29877	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I: L/A:N **6,5 MEDIUM**	LOW;LOW;none	Missing Authentication for Critical Function - Affected devices allow unauthenticated access to the web interface configuration area.	This could allow an attacker to extract internal configuration details or to reconfigure network settings.	EAVESDROPPING

SICAM P850 ———— SICAM P855	CVE-2022-29878	https://nvd.nist.gov/vuln/detail/CVE-2022-29878	AV:N/AC:H/PR:N/UI:N/S:U/C:H/I: H/A:H **8,1 HIGH**	HIGH;HIGH;HIGH	Authentication Bypass by Capture-replay - Affected devices use a limited range for challenges that are sent during the unencrypted challenge- response communication.	An unauthenticated attacker could capture a valid challenge- response pair generated by a legitimate user, and request the webpage repeatedly to wait for the same challenge to reappear for which the correct response is known. This could allow the attacker to access the management interface of the device.	ACCESS
SICAM P850 ———— SICAM P855	CVE-2022-29879	https://nvd.nist.gov/vuln/detail/CVE-2022-29879	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I: N/A:N **6,5 MEDIUM**	HIGH;none;none	Missing Authentication for Critical Function - The web based management interface of affected devices does not employ special access protection for certain internal developer views.	This could allow authenticated users to access critical device information.	EAVESDROPPING
SICAM P850 ———— SICAM P855	CVE-2022-29880	https://nvd.nist.gov/vuln/detail/CVE-2022-29880	AV:N/AC:L/PR:L/UI:R/S:C/C:L/I: L/A:N **5,4 MEDIUM**	LOW;LOW;none	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') - Affected devices do not properly validate input in the configuration interface.	This could allow an authenticated attacker to place persistent XSS attacks to perform arbitrary actions in the name of a logged user which accesses the affected views.	ACCESS
SICAM P850 ———— SICAM P855	CVE-2022-29881	https://nvd.nist.gov/vuln/detail/CVE-2022-29881	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I: N/A:N **5,3 MEDIUM**	LOW;none;none	Missing Authentication for Critical Function - The web based management interface of affected devices does not employ special access protection for certain internal developer views.	This could allow unauthenticated users to extract internal configuration details.	EAVESDROPPING
SICAM P850 ———— SICAM P855	CVE-2022-29882	https://nvd.nist.gov/vuln/detail/CVE-2022-29882	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I: L/A:N **6,1 MEDIUM**	LOW;LOW;none	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') - Affected devices do not handle uploaded files correctly.	An unauthenticated attacker could take advantage of this situation to store an XSS attack, which could - when a legitimate user accesses the error logs - perform arbitrary actions in the name of the user.	COMMAND INJECTION
SICAM P850 ———— SICAM P855	CVE-2022-29883	https://nvd.nist.gov/vuln/detail/CVE-2022-29883	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I: L/A:N **5,3 MEDIUM**	none;LOW;none	Improper Authentication - Affected devices do not restrict unauthenticated access to certain pages of the web interface.	This could allow an attacker to delete log files without authentication.	FALSE DATA INJECTION

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	CVE-2022-30228	https://nvd.nist.gov/vuln/detail/CVE-2022-30228	AV:N/AC:L/PR:N/UI:R/S:U/C:N/I: H/A:N **6,5 MEDIUM**	none;HIGH;none	Origin Validation Error - does not apply cross-origin resource sharing (CORS) restrictions for critical operations	In case an attacker tricks a legitimate user into accessing a special resource a malicious request could be executed.	OTHER
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	CVE-2022-30229	https://nvd.nist.gov/vuln/detail/CVE-2022-30229	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I: L/A:N **5,3 MEDIUM**	none;LOW;none	Missing Authentication for Critical Function	This could allow an unauthenticated attacker to change data of an user, such as credentials, in case that user's id is known.	ACCESS
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	CVE-2022-30230	https://nvd.nist.gov/vuln/detail/CVE-2022-30230	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I: H/A:H **9,8 CRITICAL**	HIGH;HIGH;HIGH	Missing Authentication for Critical Function	This could allow an unauthenticated attacker to create a new user with administrative permissions.	ACCESS
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	CVE-2022-30231	https://nvd.nist.gov/vuln/detail/CVE-2022-30231	AV:N/AC:L/PR:L/UI:N/S:U/C:L/I: N/A:N **4,3 MEDIUM**	LOW;none;none	Transmission of Private Resources into a New Sphere ('Resource Leak') - The affected software discloses password hashes of other users upon request	This could allow an authenticated user to retrieve another users password hash.	EAVESDROPPING

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 ——————————— Siemens SIMATIC S7-1500 Software Controller	CVE-2022-30694	https://nvd.nist.gov/vuln/detail/CVE-2022-30694	AV:N/AC:L/PR:N/UI:R/S:U/C:H/I: N/A:N **6,5 MEDIUM** ---> SIEMENS AV:N/AC:L/PR:L/UI:R/S:U/C:L/I: N/A:N **3,5 LOW** ---> NIST	LOW;none;none	Cross-Site Request Forgery (CSRF) - login endpoint /FormLogin in affected web services does not apply proper origin checking	could allow authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack	EAVESDROPPING
Siemens SICAM GridEdge Essential ARM Siemens SICAM GridEdge Essential GDS ARM	CVE-2022-34464	https://nvd.nist.gov/vuln/detail/CVE-2022-34464	AV:L/AC:L/PR:L/UI:N/S:U/C:N/I: H/A:N **5,5 MEDIUM**	none;HIGH;none	Exposure of Resource to Wrong Sphere - Affected software uses an improperly protected file to import SSH keys	Attackers with access to the filesystem of the host on which SICAM GridEdge runs, are able to inject a custom SSH key to that file.	FALSE DATA INJECTION
ABB zenon 7.50 ABB zenon 7.60 ABB zenon 8.00 ABB zenon 8.10 ABB zenon 8.20	CVE-2022-34836	https://nvd.nist.gov/vuln/detail/CVE-2022-34836	AV:A/AC:H/PR:N/UI:N/S:U/C:H/I: L/A:N **5,9 MEDIUM ---> ABB** AV:N/AC:L/PR:N/UI:N/S:U/C:H/I: L/A:N **8,2 HIGH** ---> NIST	HIGH;LOW;none	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') - allows the user to access files on the Zenon system and user also can add own log messages and e.g., flood the log entries.	An attacker who successfully exploit the vulnerability could access the Zenon runtime activities such as the start and stop of various activity and the last error code etc.	EAVESDROPPING
ABB zenon 7.50 ABB zenon 7.60 ABB zenon 8.00 ABB zenon 8.10 ABB zenon 8.20	CVE-2022-34837	https://nvd.nist.gov/vuln/detail/CVE-2022-34837	AV:L/AC:H/PR:N/UI:N/S:U/C:H/I: L/A:L **6,2 MEDIUM ---> ABB** AV:L/AC:L/PR:L/UI:N/S:U/C:H/I: L/A:N **6,1 MEDIUM** ---> NIST	HIGH;LOW;LOW	Insufficiently Protected Credentials - Storing Passwords in a Recoverable Format	allows an attacker who successfully exploit the vulnerability may add more network clients that may monitor various activities of the Zenon.	FALSE DATA INJECTION

ABB zenon 7.50 ABB zenon 7.60 ABB zenon 8.00 ABB zenon 8.10 ABB zenon 8.20	CVE-2022-34838	https://nvd.nist.gov/vuln/detail/CVE-2022-34838	AV:L/AC:H/PR:N/UI:N/S:C/C:H/I: H/A:H **8,1 HIGH —> ABB** AV:L/AC:L/PR:L/UI:N/S:C/C:H/I: H/A:N **8,4 HIGH** —> NIST	HIGH;HIGH;HIGH	Insufficiently Protected Credentials - Storing Passwords in a Recoverable Format	allows an attacker who successfully exploit the vulnerability may add or alter data points and corresponding attributes. Once such engineering data is used the data visualization will be altered for the end user.	FALSE DATA INJECTION
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	CVE-2022-38184	https://nvd.nist.gov/vuln/detail/CVE-2022-38184	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I: N/A:N **7,5 HIGH**	HIGH;none;none	Improper access control vulnerability	which could allow a remote, unauthenticated attacker to access an API that may induce Esri Portal for ArcGIS to read arbitrary URLs.	OTHER
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	CVE-2022-38186	https://nvd.nist.gov/vuln/detail/CVE-2022-38186	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I: L/A:L **7,1 HIGH** —> ESRI AV:N/AC:L/PR:N/UI:R/S:C/C:L/I: L/A:N **6,1 MEDIUM** —>NIST	LOW;LOW;LOW	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') - reflected XSS	may allow a remote attacker able to convince a user to click on a crafted link which could potentially execute arbitrary JavaScript code in the victim's browser.	OTHER
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	CVE-2022-38187	https://nvd.nist.gov/vuln/detail/CVE-2022-38187	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I: N/A:N **7,5 HIGH**	HIGH;none;none	Server-Side Request Forgery (SSRF)	could allow an unauthenticated attacker to induce Esri Portal for ArcGIS to read arbitrary URLs. Then, the attacker could go on to get information, perform DoS, RSSF, etc	EAVESDROPPING DENIAL OF SERVICE
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	CVE-2022-38188	https://nvd.nist.gov/vuln/detail/CVE-2022-38188	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I: L/A:L **7,1 HIGH** —> ESRI AV:N/AC:L/PR:N/UI:R/S:C/C:L/I: L/A:N **6,1 MEDIUM** —>NIST	LOW;LOW;LOW	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') - reflected XSS	may allow a remote attacker able to convince a user to click on a crafted link which could potentially execute arbitrary JavaScript code in the victim's browser.	OTHER

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	CVE-2022-38190	https://nvd.nist.gov/vuln/detail/CVE-2022-38190	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I: L/A:N **6,1 MEDIUM**	LOW;LOW;none	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') - stored Cross Site Scripting (XSS)	may allow a remote, unauthenticated attacker to pass and store malicious strings via crafted queries which when accessed could potentially execute arbitrary JavaScript code in the user's browser	OTHER
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	CVE-2022-38191	https://nvd.nist.gov/vuln/detail/CVE-2022-38191	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I: L/A:N **6,1 MEDIUM** —> ESRI AV:N/AC:L/PR:L/UI:R/S:C/C:L/I: L/A:N **5,4 MEDIUM** —> NIST	LOW;LOW;none	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	which may allow a remote, authenticated attacker to inject HTML into some locations in the home application.	FALSE DATA INJECTION
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	CVE-2022-38192	https://nvd.nist.gov/vuln/detail/CVE-2022-38192	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I: L/A:N **6,1 MEDIUM** —> ESRI AV:N/AC:L/PR:L/UI:R/S:C/C:L/I: L/A:N **5,4 MEDIUM** —> NIST	LOW;LOW;none	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') - stored Cross Site Scripting (XSS)	may allow a remote, authenticated attacker to pass and store malicious strings via crafted queries which when accessed could potentially execute arbitrary JavaScript code in the user's browser	OTHER
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	CVE-2022-38193	https://nvd.nist.gov/vuln/detail/CVE-2022-38193	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I: L/A:N **6,1 MEDIUM** —> ESRI AV:N/AC:L/PR:N/UI:R/S:C/C:H/I: H/A:H **9,6 CRITICAL** —> NIST	LOW;LOW;none	Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')	may allow a remote, unauthenticated attacker to pass strings which could potentially cause arbitrary code execution	COMMAND INJECTION
Esri Portal For Arcgis 10.8.1 Esri Portal For Arcgis 10.8.1 on x64	CVE-2022-38194	https://nvd.nist.gov/vuln/detail/CVE-2022-38194	AV:L/AC:L/PR:H/UI:N/S:C/C:H/I: L/A:N **6,7 MEDIUM** —> ESRI AV:L/AC:L/PR:L/UI:N/S:U/C:H/I: N/A:N **5,5 MEDIUM** —> NIST	HIGH;LOW;none	Missing Encryption of Sensitive Data - a system property is not properly encrypted	This may lead to a local user reading sensitive information from a properties file.	EAVESDROPPING

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	CVE-2022-38195	https://nvd.nist.gov/vuln/detail/CVE-2022-38195	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I: L/A:N **6,1 MEDIUM**	LOW;LOW;none	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	may allow a **remote** **unauthorized** attacker able to convince a user to click on a crafted link which could potentially execute arbitrary JavaScript code in the victim's browser.	OTHER
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	CVE-2022-38196	https://nvd.nist.gov/vuln/detail/CVE-2022-38196	AV:N/AC:L/PR:H/UI:N/S:U/C:N/I: H/A:H **6,5 MEDIUM** —> ESRI AV:N/AC:L/PR:L/UI:N/S:U/C:N/I: H/A:H **8,1 HIGH** —> NIST	none;HIGH;HIGH	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	may result in a denial of service by allowing a remote, **authenticated** attacker to overwrite internal ArcGIS Server directory	DENIAL OF SERVICE

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	CVE-2022-38197	https://nvd.nist.gov/vuln/detail/CVE-2022-38197	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I: L/A:N **6,1 MEDIUM**	LOW;LOW;none	URL Redirection to Untrusted Site ('Open Redirect')	may allow a remote, unauthenticated attacker to phish a user into accessing an attacker controlled website via a crafted query parameter. It could lead to credential theft, malware distribution or other advanced attack	OTHER
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	CVE-2022-38198	https://nvd.nist.gov/vuln/detail/CVE-2022-38198	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I: L/A:N **6,1 MEDIUM**	LOW;LOW;none	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	may allow a remote, **unauthenticated** attacker to convince a user to click on a crafted link which could potentially execute arbitrary JavaScript code in the victim's browser	OTHER
Esri ArcGIS Server 10.7.1 on X64 Esri ArcGIS Server 10.8.1 on X64 Esri ArcGIS Server 10.9.1 on X64	CVE-2022-38199	https://nvd.nist.gov/vuln/detail/CVE-2022-38199	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I: L/A:N **6,1 MEDIUM**	LOW;LOW;none	Download of Code Without Integrity Check	may in some edge cases allow a remote, unauthenticated attacker to induce an unsuspecting victim to launch a process in the victim's PATH environment.	OTHER
Esri ArcGIS Server 10.7.1 Esri ArcGIS Server 10.8.1 Esri ArcGIS Server 10.7.1 on X64 Esri ArcGIS Server 10.8.1 on X64	CVE-2022-38200	https://nvd.nist.gov/vuln/detail/CVE-2022-38200	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I: L/A:N **6,1 MEDIUM**	LOW;LOW;none	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Specifically crafted web requests can execute arbitrary JavaScript in the context of the victim's browser.	OTHER

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	CVE-2022-38202	https://nvd.nist.gov/vuln/detail/CVE-2022-38202	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I: N/A:N **7,5 HIGH**	HIGH;none;none	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	may allow a remote, unauthenticated attacker traverse the file system to access files outside of the intended directory on ArcGIS Server. This could lead to the disclosure of sensitive site configuration information (not user datasets).	EAVESDROPPING
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	CVE-2022-38203	https://nvd.nist.gov/vuln/detail/CVE-2022-38203	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I: N/A:N **7,5 HIGH**	HIGH;none;none	Protections against potential Server-Side Request Forgery (SSRF) were not fully honored	may allow a remote, unauthenticated attacker to forge requests to arbitrary URLs from the system, potentially leading to network enumeration or reading from hosts inside the network perimeter,	EAVESDROPPING
Esri Portal For Arcgis 10.7.1 Esri Portal For Arcgis 10.8.1 Esri Portal For Arcgis 10.8.1 on x64	CVE-2022-38204	https://nvd.nist.gov/vuln/detail/CVE-2022-38204	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I: L/A:N **6,1 MEDIUM**	LOW;LOW;none	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') - reflected XSS	may allow a remote, unauthenticated attacker to create a crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim's browser	OTHER

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	CVE-2022-38205	https://nvd.nist.gov/vuln/detail/CVE-2022-38205	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I: N/A:N **7,5 HIGH**	HIGH;none;none	directory traversal issue	may allow a remote, unauthenticated attacker to traverse the file system and lead to the disclosure of sensitive data (not customer-published content)	EAVESDROPPING
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	CVE-2022-38206	https://nvd.nist.gov/vuln/detail/CVE-2022-38206	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I: L/A:N **6,1 MEDIUM**	LOW;LOW;none	reflected XSS vulnerability	may allow a remote remote, unauthenticated attacker to create a crafted link which when clicked could execute arbitrary JavaScript code in the victim's browser.	OTHER
Esri Portal For Arcgis 10.7.1 Esri Portal For Arcgis 10.8.1 Esri Portal For Arcgis 10.8.1 on x64	CVE-2022-38207	https://nvd.nist.gov/vuln/detail/CVE-2022-38207	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I: L/A:N **6,1 MEDIUM**	LOW;LOW;none	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') - reflected XSS	may allow a remote remote, unauthenticated attacker to create a crafted link which when clicked which could execute arbitrary JavaScript code in the victim's browser.	OTHER

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	CVE-2022-38208	https://nvd.nist.gov/vuln/detail/CVE-2022-38208	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I: L/A:N **6,1 MEDIUM**	LOW;LOW;none	URL Redirection to Untrusted Site ('Open Redirect')	may allow a remote, unauthenticated attacker to craft a URL that could redirect a victim to an arbitrary website, simplifying phishing attacks.	OTHER
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	CVE-2022-38209	https://nvd.nist.gov/vuln/detail/CVE-2022-38209	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I: L/A:N **6,1 MEDIUM**	LOW;LOW;none	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') - reflected XSS	which may allow a remote, unauthenticated attacker to create a crafted link which when clicked could execute arbitrary JavaScript code in the victim's browser.	OTHER
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	CVE-2022-38210	https://nvd.nist.gov/vuln/detail/CVE-2022-38210	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I: L/A:N **6,1 MEDIUM**	LOW;LOW;none	reflected HTML injection vulnerability	may allow a remote, unauthenticated attacker to create a crafted link which when clicked could render arbitrary HTML in the victim's browser.	OTHER

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	CVE-2022-38211	https://nvd.nist.gov/vuln/detail/CVE-2022-38211	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I: N/A:N **7,5 HIGH**	HIGH;none;none	Protections against potential Server-Side Request Forgery (SSRF) vulnerabilities in Esri Portal for ArcGIS versions 10.9.1 and below were not fully honored	may allow a remote, unauthenticated attacker to forge requests to arbitrary URLs from the system, potentially leading to network enumeration or reading from hosts inside the network perimeter	EAVESDROPPING
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	CVE-2022-38212	https://nvd.nist.gov/vuln/detail/CVE-2022-38212	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I: N/A:N **7,5 HIGH**	HIGH;none;none	Protections against potential Server-Side Request Forgery (SSRF) vulnerabilities in Esri Portal for ArcGIS versions 10.8.1 and below were not fully honored	may allow a remote, unauthenticated attacker to forge requests to arbitrary URLs from the system, potentially leading to network enumeration or reading from hosts inside the network perimeter,	EAVESDROPPING
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	CVE-2022-38465	https://nvd.nist.gov/vuln/detail/CVE-2022-38465	AV:L/AC:L/PR:N/UI:N/S:C/C:H/I: H/A:H **9,3 CRITICAL** —> SIEMENS AV:L/AC:L/PR:L/UI:N/S:U/C:H/I: H/A:H **7,8 HIGH** —> NIST	HIGH;HIGH;HIGH	Insufficiently Protected Credentials	could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication.	EAVESDROPPING
SICAM P850 ———— SICAM P855	CVE-2022-40226	https://nvd.nist.gov/vuln/detail/CVE-2022-40226	AV:N/AC:H/PR:N/UI:R/S:U/C:H/I: H/A:H **7,5 HIGH—> SIEMENS** AV:N/AC:L/PR:L/UI:N/S:U/C:H/I: H/A:N **8,1 HIGH** —> NIST	HIGH;HIGH;HIGH	Session Fixation - Affected devices accept user defined session cookies and do not renew the session cookie after login/logout.	This could allow an attacker to take over another user's session after login.	ACCESS

SICAM P850 ———— SICAM P855	CVE-2022-41665	https://nvd.nist.gov/vuln/detail/CVE-2022-41665	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I: H/A:H **9,8 CRITICAL —> SIEMENS** AV:N/AC:L/PR:L/UI:N/S:U/C:H/I: H/A:H **8,8 HIGH** —> NIST	HIGH;HIGH;HIGH	Improper Neutralization of Parameter/Argument Delimiters - Affected devices do not properly validate the parameter of a specific GET request.	This could allow an unauthenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device.	COMMAND INJECTION DENIAL OF SERVICE
Siemens (SICAM Q100) 7KG9501-0AA31-2AA1 ——— SICAM Q200	CVE-2022-43398	https://nvd.nist.gov/vuln/detail/CVE-2022-43398	AV:N/AC:H/PR:N/UI:R/S:U/C:H/I: H/A:H **7,5 HIGH** —> SIEMENS AV:N/AC:L/PR:N/UI:R/S:U/C:H/I: H/A:H **8,8 HIGH** —> NIST	HIGH;HIGH;HIGH	Session Fixation - Affected devices do not renew the session cookie after login/logout and also accept user defined session cookies	An attacker could overwrite the stored session cookie of a user. After the victim logged in, the attacker is given access to the user's account through the activated session.	ACCESS
Siemens (SICAM Q100) 7KG9501-0AA31-2AA1 ————— SICAM P850 ——— SICAM Q200 ———— SICAM P855	CVE-2022-43439	https://nvd.nist.gov/vuln/detail/CVE-2022-43439	AV:N/AC:L/PR:L/UI:N/S:C/C:H/I: H/A:H **9,9 CRITICAL —> SIEMENS** AV:N/AC:L/PR:L/UI:N/S:U/C:H/I: H/A:H **8,8 HIGH** —> NIST	HIGH;HIGH;HIGH	Improper Input Validation - do not properly validate the Language-parameter in requests to the web interface on port 443/tcp	This could allow an authenticated remote attacker to crash the device (followed by an automatic reboot) or to execute arbitrary code on the device.	COMMAND INJECTION DENIAL OF SERVICE
Siemens (SICAM Q100) 7KG9501-0AA31-2AA1 ————— SICAM P850 ——— SICAM Q200 ———— SICAM P855	CVE-2022-43545	https://nvd.nist.gov/vuln/detail/CVE-2022-43545	AV:N/AC:L/PR:L/UI:N/S:C/C:H/I: H/A:H **9,9 CRITICAL —> SIEMENS** AV:N/AC:L/PR:L/UI:N/S:U/C:H/I: H/A:H **8,8 HIGH —> NIST**	HIGH;HIGH;HIGH	Improper Input Validation - Affected devices do not properly validate the RecordType- parameter in requests to the web interface on port 443/tcp	This could allow an authenticated remote attacker to crash the device (followed by an automatic reboot) or to execute arbitrary code on the device.	COMMAND INJECTION DENIAL OF SERVICE
Siemens (SICAM Q100) 7KG9501-0AA31-2AA1 ————— SICAM P850 ——— SICAM Q200 ———— SICAM P855	CVE-2022-43546	https://nvd.nist.gov/vuln/detail/CVE-2022-43546	AV:N/AC:L/PR:L/UI:N/S:C/C:H/I: H/A:H **9,9 CRITICAL —> SIEMENS** AV:N/AC:L/PR:L/UI:N/S:U/C:H/I: H/A:H **8,8 HIGH —> NIST**	HIGH;HIGH;HIGH	Improper Input Validation - Affected devices do not properly validate the EndTime-parameter in requests to the web interface on port 443/tcp.	This could allow an authenticated remote attacker to crash the device (followed by an automatic reboot) or to execute arbitrary code on the device.	COMMAND INJECTION DENIAL OF SERVICE
Siemens SICAM PAS (Power Automation System) ————— Siemens SICAM PQS	CVE-2022-43722	https://nvd.nist.gov/vuln/detail/CVE-2022-43722	AV:L/AC:L/PR:N/UI:R/S:U/C:H/I: H/A:H **7,8 HIGH**	HIGH;HIGH;HIGH	Uncontrolled Search Path Element	This could allow an attacker to place a custom malicious DLL in this folder which is then run with SYSTEM rights when a service is started that requires this DLL.	LATERAL MOVEMENT / PRIVILEGE ESCALATION PERSISTENCE

Siemens SICAM PAS (Power Automation System) ------------------- Siemens SICAM PQS	CVE-2022-43724	https://nvd.nist.gov/vuln/detail/CVE-2022-43724	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I: H/A:H **9,8 CRITICAL**	HIGH;HIGH;HIGH	Cleartext Transmission of Sensitive Information	transmits the database credentials for the inbuilt SQL server in cleartext. In combination with the by default enabled xp_cmdshell feature unauthenticated remote attackers could execute custom OS commands	COMMAND INJECTION
SIPROTEC	CVE-2022-45044	https://nvd.nist.gov/vuln/detail/CVE-2022-45044	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I: N/A:H **7,5 HIGH** —> NIST AV:N/AC:L/PR:N/UI:N/S:U/C:N/I: N/A:L **5,3 MEDIUM** —> SIEMENS	none;none;HIGH	Uncontrolled Resource Consumption - Affected devices do not properly restrict secure client-initiated renegotiations within the SSL and TLS protocols.	This could allow an attacker to create a denial of service condition on the ports 443/tcp and 4443/tcp for the duration of the attack.	DENIAL OF SERVICE
Esri Portal For Arcgis 10.9.1 Esri Portal For Arcgis 10.9.1 on x64 Esri Portal For Arcgis 11.0	CVE-2023-25829	https://nvd.nist.gov/vuln/detail/CVE-2023-25829	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I: L/A:N **6,1 MEDIUM**	LOW;LOW;none	URL Redirection to Untrusted Site ('Open Redirect')	may allow a remote, unauthenticated attacker to craft a URL that could redirect a victim to an arbitrary website, simplifying phishing attacks.	OTHER
Esri Portal For Arcgis 10.7.1 Esri Portal For Arcgis 10.8.1 Esri Portal For Arcgis 10.8.1 on x64 Esri Portal For Arcgis 10.9.1 Esri Portal For Arcgis 10.9.1 on x64	CVE-2023-25830	https://nvd.nist.gov/vuln/detail/CVE-2023-25830	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I: L/A:N **6,1 MEDIUM**	LOW;LOW;none	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') - reflected XSS	may allow a remote, unauthenticated attacker to create a crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim’s browser.	OTHER
Esri Portal For Arcgis 10.7.1 Esri Portal For Arcgis 10.8.1 Esri Portal For Arcgis 10.8.1 on x64 Esri Portal For Arcgis 10.9.1 Esri Portal For Arcgis 10.9.1 on x64	CVE-2023-25831	https://nvd.nist.gov/vuln/detail/CVE-2023-25831	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I: L/A:N **6,1 MEDIUM**	LOW;LOW;none	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') - reflected XSS	may allow a remote, unauthenticated attacker to create a crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim’s browser.	OTHER

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	CVE-2023-25832	https://nvd.nist.gov/vuln/detail/CVE-2023-25832	AV:N/AC:L/PR:N/UI:R/S:U/C:H/I: H/A:H **8,8 HIGH**	HIGH;HIGH;HIGH	cross-site-request forgery vulnerability	may allow an attacker to trick an authorized user into executing unwanted actions	COMMAND INJECTION
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	CVE-2023-25833	https://nvd.nist.gov/vuln/detail/CVE-2023-25833	AV:N/AC:L/PR:L/UI:R/S:C/C:L/I: L/A:N **5,4 MEDIUM**	LOW;LOW;none	HTML injection vulnerability	may allow a remote, authenticated attacker to create a crafted link which when clicked could render arbitrary HTML in the victim's browser (no stateful change made or customer data rendered).	OTHER
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	CVE-2023-25834	https://nvd.nist.gov/vuln/detail/CVE-2023-25834	AV:N/AC:L/PR:L/UI:N/S:U/C:L/I: L/A:N **5,4 MEDIUM**	LOW;LOW;none	Improper Privilege Management	may allow users to access content that they are no longer privileged to access.	LATERAL MOVEMENT / PRIVILEGE ESCALATION

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	CVE-2023-25835	https://nvd.nist.gov/vuln/detail/CVE-2023-25835	AV:N/AC:L/PR:H/UI:R/S:C/C:L/I: L/A:N **4,8 MEDIUM**	LOW;LOW;none	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	The attack could disclose a privileged token which may result the attacker gaining full control of the Portal.	ACCESS
Esri Portal For Arcgis 10.7.1 Esri Portal For Arcgis 10.8.1 Esri Portal For Arcgis 10.8.1 on x64 Esri Portal For Arcgis 10.9.1 Esri Portal For Arcgis 10.9.1 on x64	CVE-2023-25836	https://nvd.nist.gov/vuln/detail/CVE-2023-25836	AV:N/AC:L/PR:L/UI:R/S:C/C:L/I: L/A:N **5,4 MEDIUM**	LOW;LOW;none	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	may allow a remote, authenticated attacker to create a crafted link which when clicked could potentially execute arbitrary JavaScript code in the victims browser	OTHER
Esri Portal For Arcgis 10.8.1 Esri Portal For Arcgis 10.8.1 on x64 Esri Portal For Arcgis 10.9	CVE-2023-25837	https://nvd.nist.gov/vuln/detail/CVE-2023-25837	AV:N/AC:L/PR:H/UI:R/S:C/C:L/I: L/A:N **4,8 MEDIUM**	LOW;LOW;none	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	may allow a remote, authenticated attacker to create a crafted link which when clicked could potentially execute arbitrary JavaScript code in the victims browser.	OTHER
ESRI ArcGIS 10.8.1	CVE-2023-25840	https://nvd.nist.gov/vuln/detail/CVE-2023-25840	AV:N/AC:L/PR:H/UI:R/S:C/C:N/I: L/A:N **3,4 LOW**	none;LOW;none	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	may allow a remote, authenticated attacker to create a crafted link which onmouseover wont execute but could potentially render an image in the victims browser	OTHER
ESRI ArcGIS 10.8.1	CVE-2023-25841	https://nvd.nist.gov/vuln/detail/CVE-2023-25841	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I: L/A:N **6,1 MEDIUM**	LOW;LOW;none	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	may allow a remote, unauthenticated attacker to create crafted content which when clicked could potentially execute arbitrary JavaScript code in the victim's browser.	OTHER
SIPROTEC	CVE-2023-28766	https://nvd.nist.gov/vuln/detail/CVE-2023-28766	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I: N/A:H **7,5 HIGH**	none;none;HIGH	NULL Pointer Dereference - Affected devices lack proper validation of http request parameters of the hosted web service	An unauthenticated remote attacker could send specially crafted packets that could cause denial of service condition of the target device.	DENIAL OF SERVICE

Siemens SIMATIC WinCC 7.4 Service Pack 1 Update 3	CVE-2023-28829	https://nvd.nist.gov/vuln/detail/CVE-2023-28829	AV:A/AC:H/PR:H/UI:N/S:U/C:L/I: L/A:L **3,9 LOW —> SIEMENS** AV:N/AC:L/PR:L/UI:N/S:U/C:H/I: H/A:H **8,8 HIGH** —> NIST	LOW;LOW;LOW	Use of Obsolete Function - legacy services (Alarms & Events)) were used per default. These services were designed on top of the Windows ActiveX and DCOM mechanisms and do not implement state-of-the-art security mechanisms for authentication and encryption of contents.	Since there is no security mechanisms an attacker could get access to everything. However, SIEMENS rates this vulnerability with low criticality	ACCESS
Siemens WinCC 7.4	CVE-2023-30897	https://nvd.nist.gov/vuln/detail/CVE-2023-30897	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I: H/A:H **7,8 HIGH**	HIGH;HIGH;HIGH	Incorrect Permission Assignment for Critical Resource - Affected applications fail to set proper access rights for their installation folder if a non-default installation path was chosen during installation	This could allow an authenticated local attacker to inject arbitrary code and escalate privileges.	COMMAND INJECTION LATERAL MOVEMENT / PRIVILEGE ESCALATION
SICAM Q200	CVE-2023-30901	https://nvd.nist.gov/vuln/detail/CVE-2023-30901	AV:N/AC:L/PR:N/UI:R/S:U/C:N/I: L/A:N **4,3 MEDIUM —> SIEMENS** AV:N/AC:L/PR:N/UI:R/S:U/C:H/I: H/A:H **8,8 HIGH** —> NIST	none;LOW;none	Cross-Site Request Forgery (CSRF) - The web interface of the affected devices are vulnerable to Cross-Site Request Forgery attacks.	By tricking an authenticated victim user to click a malicious link, an attacker could perform arbitrary actions on the device on behalf of the victim user.	COMMAND INJECTION
SICAM Q200	CVE-2023-31238	https://nvd.nist.gov/vuln/detail/CVE-2023-31238	AV:N/AC:H/PR:L/UI:R/S:C/C:L/I: L/A:L **5,5 MEDIUM —> SIEMENS** AV:N/AC:H/PR:N/UI:N/S:U/C:L/I: L/A:N **4,8 MEDIUM** —> NIST	LOW;LOW;LOW	Incorrect Permission Assignment for Critical Resource - Affected devices are missing cookie protection flags when using the default settings	An attacker who gains access to a session token can use it to impersonate a legitimate application user	ACCESS

ABB zenon 7.50 ABB zenon 7.60 ABB zenon 8.00 ABB zenon 8.10 ABB zenon 8.20	CVE-2023-3321	https://nvd.nist.gov/vuln/detail/CVE-2023-3321	AV:L/AC:H/PR:L/UI:N/S:U/C:H/I: H/A:H **7,0 HIGH —> ABB** AV:N/AC:L/PR:L/UI:N/S:U/C:H/I: H/A:H **8,8 HIGH —> NIST**	HIGH;HIGH;HIGH	External Control of System or Configuration Setting - allowing low-privileged users to read and update the data in various directories used by the Zenon system	An attacker could exploit the vulnerability by using specially crafted programs to exploit the vulnerabilities by allowing them to run on the zenon installed hosts. Subsequently, a successful exploit could allow attackers to execute programs on the zenon system. While the attackers need internal information from the zenon system and need to access the system via various means some of the zenon directories are accessible for low privileged users. These directories may be used further to carry out the attacks.	FALSE DATA INJECTION EAVESDROPPING
ABB zenon 7.50 ABB zenon 7.60 ABB zenon 8.00 ABB zenon 8.10 ABB zenon 8.20	CVE-2023-3322	https://nvd.nist.gov/vuln/detail/CVE-2023-3322	AV:L/AC:H/PR:L/UI:N/S:U/C:H/I: H/A:H **7,0 HIGH —> ABB** AV:N/AC:L/PR:L/UI:N/S:U/C:H/I: H/A:N **8,1 HIGH** —> NIST	HIGH;HIGH;HIGH	Incorrect Permission Assignment for Critical Resource - allowing low-privileged users to read and update the data in various directories used by the Zenon system	An attacker could exploit the vulnerability by using specially crafted programs to exploit the vulnerabilities by allowing them to run on the zenon installed hosts. Subsequently, a successful exploit could allow attackers to execute programs on the zenon system. While the attackers need internal information from the zenon system and need to access the system via various means some of the zenon directories are accessible for low privileged users. These directories may be used further to carry out the attacks.	FALSE DATA INJECTION EAVESDROPPING

ABB zenon 7.50 ABB zenon 7.60 ABB zenon 8.00 ABB zenon 8.10 ABB zenon 8.20	CVE-2023-3323	https://nvd.nist.gov/vuln/detail/CVE-2023-3323	AV:P/AC:H/PR:L/UI:N/S:U/C:L/I: H/A:H **5,9 MEDIUM —> ABB** AV:N/AC:L/PR:L/UI:N/S:U/C:L/I: L/A:N **5,4 MEDIUM** —> NIST	LOW;HIGH;HIGH	Incorrect Default Permissions - allowing low-privileged users to read and update the data in various directories used by the Zenon system	An attacker could exploit the vulnerability by using specially crafted programs to exploit the vulnerabilities by allowing them to run on the zenon installed hosts. Subsequently, a successful exploit could allow attackers to execute programs on the zenon system. While the attackers need internal information from the zenon system and need to access the system via various means some of the zenon directories are accessible for low privileged users. These directories may be used further to carry out the attacks.	FALSE DATA INJECTION EAVESDROPPING
ABB zenon 7.50 ABB zenon 7.60 ABB zenon 8.00 ABB zenon 8.10 ABB zenon 8.20	CVE-2023-3324	https://nvd.nist.gov/vuln/detail/CVE-2023-3324	AV:L/AC:H/PR:L/UI:R/S:U/C:L/I: H/A:H **6,3 MEDIUM —> ABB** AV:N/AC:H/PR:L/UI:N/S:U/C:H/I: H/A:H **7,5 HIGH** —> NIST	LOW;HIGH;HIGH	Deserialization of Untrusted Data - allowing low-privileged users to read and update the data in various directories used by the Zenon system	An attacker could exploit the vulnerability by using specially crafted programs to exploit the vulnerabilities by allowing them to run on the zenon installed hosts. Subsequently, a successful exploit could allow attackers to execute programs on the zenon system. While the attackers need internal information from the zenon system and need to access the system via various means some of the zenon directories are accessible for low privileged users. These directories may be used further to carry out the attacks.	FALSE DATA INJECTION EAVESDROPPING