CPE product affected	CVE id	CVE link	CVSS - vector and score	CIA	Description of the vulnerability	What could an attacker achieve?	Capabilities
						allows local users to gain privileges	
			AV:L/AC:L/Au:N/C:C/I:C/			via format string specifiers in the	
	CVE-2005-	https://nvd.nist.	A:C	HIGH;HIGH;HIG		ARCHOME environment variable to	LATERAL MOVEMENT /
ESRI ArcGIS 9.0	1394	gov/vuln/detail/CVE-2005-1394	7,2 HIGH	Н	Format string vulnerability	(1) wservice or (2) lockmgr	PRIVILEGE ESCALATION
			,		,	, , ,	
						allows remote attackers to cause a	
ESRI ArcGIS ESRI ArcGIS 9.0						denial of service (crash) and	
ESRI ArcGIS 10.0.2.3200						possibly execute arbitrary code via a	
ESRI ArcGIS 10.1						large number that requires more than	
ESRI ArcGIS 10.2			AV:N/AC:L/Au:N/C:L/I:L/		Improper Restriction of Operations	8 bytes to represent in ASCII, which	
ESRI ArcGIS 10.8.1	CVE-2007-	https://nvd.nist.	A:L	LOW;LOW;LO	within the Bounds of a Memory	triggers the overflow in an sprintf	COMMAND INJECTION
ESRI ArcGIS 11.1	4278	gov/vuln/detail/CVE-2007-4278	7,5 HIGH	W	Buffer	function call.	DENIAL OF SERVICE
						uses a hard-coded password, which	
						allows local users to access a back-	
			AV:N/AC:L/PR:N/UI:N/S:			end database and gain privileges, as	EAV/ESDBODDING
Siemens SIMATIC WinCC 7.4	CVE-2010-	https://nvd.nist.	C/C:H/I: H/A:H	HIGH:HIGH:HIG		demonstrated in the wild in July	LATERAL MOVEMENT /
Service Pack 1 Update 3	2772	gov/vuln/detail/CVE-2010-2772	10,0 CRITICAL	H	Credentials Management Errors	2010 by the Stuxnet worm	PRIVILEGE ESCALATION
Service Fack 1 Opuate 5	2112	gov/vum/detaii/CVL-2010-2112	10,0 CRITICAL	11	, and the second	2010 by the Stuxhet worth	FRIVILLOL LOCALATION
					Improper Control of Generation of		
			AV:N/AC:M/Au:N/C:C/I:C/		Code ('Code Injection') - does not	allows user-assisted remote	
ESRI ArcGIS ESRI ArcGIS 9.0	CVE-2012-	https://nvd.nist	A:C	HIGH;HIGH;HIG	properly prompt users before	attackers to execute arbitrary VBA	
ESRI ArcGIS 10.0.2.3200	1661	gov/vuln/detail/CVE-2012-1661	9,3 HIGH	Н	executing embedded VBA macros	code via a crafted map (. mxd) file	COMMAND INJECTION
						allows remote authenticated users to	ļ
			AV:N/AC:L/Au:S/C:P/I:P/		Improper Neutralization of Special	execute arbitrary SQL commands via	
	CVE-2012-	https://nvd.nist.	A:P	LOW;LOW;LO	' '	the where parameter to a query URI	
ESRI ArcGIS 10.1	4949	gov/vuln/detail/CVE-2012-4949	6,5 MEDIUM	W	('SQL Injection')	for a REST service.	COMMAND INJECTION
			-,-		, , ,		
						allows remote authenticated users to	
	01/5 00/0		AV:N/AC:M/Au:S/C:N/I:P/			upload .exe files by leveraging (1)	
	CVE-2013-	https://nvd.nist.	A:N	none;LOW;non		publisher or (2) administrator	
ESRI ArcGIS 10.1	5221	gov/vuln/detail/CVE-2013-5221	3,5 LOW	е	Improper Input Validation	privileges.	COMMAND INJECTION
			AV:N/AC:M/Au:S/C:N/I:P/		Improper Neutralization of Input	allow remote authenticated users to	
	CVE-2013-	https://nvd.nist.	A:N	none;LOW;non	During Web Page Generation ('Cross-	inject arbitrary web script or HTML	
ESRI ArcGIS 10.1	5222	gov/vuln/detail/CVE-2013-5222	3,5 LOW	e	site Scripting')	via unspecified vectors.	COMMAND INJECTION
			AV:N/AC:L/PR:N/UI:N/S:		Improper Authentication - do not	allows remote attackers to bypass	
	CVE-2013-	https://nvd.nist.	C/C:H/I: H/A:H	HIGH;HIGH;HIG	· ·	intended access restrictions via TCP	
Siemens SINAMICS G120	6920	gov/vuln/detail/CVE-2013-6920	10,0 CRITICAL	Н	TELNET sessions	traffic to port (1) 21 or (2) 23.	ACCESS
-							
FCDI A == CIC 40.4	C)/E 2012	https://prod.pist	AV:N/AC:M/Au:S/C:N/I:P/	nanad OWG	Improper Neutralization of Input	allows remote authenticated users to	
ESRI ArcGIS 10.1	CVE-2013-	https://nvd.nist	A:N	none;LOW;non	During Web Page Generation ('Cross-	'	COMMAND IN ICCTION
ESRI ArcGIS 10.2	7231	gov/vuln/detail/CVE-2013-7231	3,5 LUW	е	site Scripting')	via unspecified vectors	COMMAND INJECTION

ESRI ArcGIS ESRI ArcGIS 9.0						allows remote attackers to execute	
ESRI ArcGIS 10.0.2.3200			AV:N/AC:L/Au:N/C:P/I:P/		Improper Neutralization of Special	arbitrary SQL commands via	COMMAND INJECTION
ESRI ArcGIS 10.1	CVE-2013-	https://nvd.nist.	A:P	LOW;LOW;LO	Elements used in an SQL Command	unspecified input to the map or	FALSE DATA INJECTION
ESRI ArcGIS 10.2	7232	gov/vuln/detail/CVE-2013-7232	7,5 HIGH	W	('SQL Injection')	feature service.	EAVESDROPPING
			AV:N/AC:M/Au:N/C:N/I:P/		Improper Neutralization of Input	allow remote attackers to inject	
	CVE-2014-	https://nvd.nist.	A:N	none;LOW;non	During Web Page Generation ('Cross-	arbitrary web script or HTML via	
ESRI ArcGIS for Server 10.1.1	5121	gov/vuln/detail/CVE-2014-5121	4,3 MEDIUM	е	site Scripting')	unspecified parameters.	COMMAND INJECTION
						allows remote attackers to redirect	
						users to arbitrary web sites and	
			AV:N/AC:M/Au:N/C:P/I:P/			conduct phishing attacks via an	
	CVE-2014-	https://nvd.nist.	A:N	LOW;LOW;non		unspecified parameter, related to	
ESRI ArcGIS for Server 10.1.1	5122	gov/vuln/detail/CVE-2014-5122	5,8 MEDIUM	е	Open redirect vulnerability	login.	OTHER
			AV:N/AC:M/Au:N/C:N/I:P/		Improper Neutralization of Input	allow remote attackers to inject	
	CVE-2014-	https://nvd.nist.	A:N	none;LOW;non	During Web Page Generation ('Cross-	•	
ESRI ArcGIS for Server 10.1.1	9741	gov/vuln/detail/CVE-2014-9741	4,3 MEDIUM	е	site Scripting')	unspecified vectors.	COMMAND INJECTION
					·		
						Specially crafted packets sent to	
						port 50000/UDP could cause a	
			A \ / \ N \ / A \ C \ \ / A \ \ N \ / C \ N \ / \ N \ /			denial-of-service of the affected	
	CVE 2015	https://nvd.nist.	AV:N/AC:L/Au:N/C:N/I:N/			device. A manual reboot may be	
SIPROTEC	CVE-2015- 5374	gov/vuln/detail/CVE-2015-5374	A:C 7.8 HIGH	none;none;HIG	Data Processing Errors	required to recover the service of the device.	DENIAL OF SERVICE
SIFROILG	3374	<u>gov/vum/uetan/CvL=2013-33/4</u>	, -	11	Data Flocessing Lilois		DENIAL OF SERVICE
	0.45 0040		AV:N/AC:L/PR:N/UI:N/S:			could allow remote attackers to	
0.00000	CVE-2016-	https://nvd.nist.	U/C:L/I: N/A:N		Exposure of Sensitive Information to	obtain sensitive device information if	
SIPROTEC	4784	gov/vuln/detail/CVE-2016-4784	5,3 MEDIUM	е	an Unauthorized Actor	network access was obtained.	EAVESDROPPING
						could allow remote attackers to	
			AV:N/AC:L/PR:N/UI:N/S:			obtain a limited amount of device	
	CVE-2016-	https://nvd.nist.	U/C:L/I: N/A:N	LOW;none;non	Exposure of Sensitive Information to	memory content if network access	
SIPROTEC	4785	gov/vuln/detail/CVE-2016-4785	5,3 MEDIUM	е	an Unauthorized Actor	was obtained	EAVESDROPPING
			AV:N/AC:L/PR:N/UI:N/S:				
Siemens SIMATIC WinCC 7.4	CVE-2016-	https://nvd.nist.	U/C:H/I: H/A:H	HIGH;HIGH;HIG		allow remote attackers to execute	
Service Pack 1 Update 3	5743	gov/vuln/detail/CVE-2016-5743	9,8 CRITICAL	Н	Improper Input Validation	arbitrary code via crafted packets.	COMMAND INJECTION
					Exposure of Sensitive Information to		
					an Unauthorized Actor & Credential		
					Management Errors - does not	makes it easier for local users to	
Siemens SICAM PAS (Power	CVE-2016-	https://nvd.nist.	AV:L/AC:L/PR:H/UI:N/S:U	HIGH;HIGH;HIG	properly restrict password data in the	calculate passwords by leveraging	LATERAL MOVEMENT
Automation System)	5848	gov/vuln/detail/CVE-2016-5848	/C:H/I: H/A:H	н	database	unspecified database privileges.	PRIVILEGE ESCALATION
·						allows local users to obtain	
Siemens SICAM PAS (Power	CVE-2016-	https://nvd.nist.	AV:L/AC:H/PR:L/UI:N/S·U	LOW:none:non	Exposure of Sensitive Information to	sensitive configuration information	
			1	1,	,		I

	CVE-2016-	https://nvd.nist.	AV:N/AC:L/PR:N/UI:N/S: U/C:H/I: H/A:H	HIGH;HIGH;HIG		could possibly circumvent authentication and perform certain	LATERAL MOVEMENT /
SIPROTEC	7112	gov/vuln/detail/CVE-2016-7112	9,8 CRITICAL	Н	Improper Authentication	administrative operations.	PRIVILEGE ESCALATION
,		,	AV:N/AC:L/PR:N/UI:N/S:		1	Specially crafted packets sent to	
•	CVE-2016-	https://nvd.nist.	U/C:N/I: N/A:H	none;none;HIG	1	port 80/tcp could cause the affected	
SIPROTEC	7113	gov/vuln/detail/CVE-2016-7113	7,5 HIGH	н	Resource Management Errors	device to go into defect mode.	DENIAL OF SERVICE
				/		could possibly circumvent	
		/		/	1	authentication and perform certain	
				/	1	administrative operations. A	
			AV:N/AC:L/PR:L/UI:N/S:	/	1	legitimate user must be logged into	
	CVE-2016-	https://nvd.nist.		HIGH;HIGH;HIG		the web interface for the attack to be	
	7114			H	Improper Authentication	successful.	ACCESS
			5,5 1			-	7.00_22
,		·	1		Improper Access Control - Unquoted		
•	1	·	1	1 '	service paths could allow local	1	
•	1	·	1	1 '	Microsoft Windows operating system	1	
Siemens SIMATIC WinCC 7.4		'	1	1 '	users to escalate their privileges if	By scalating privileges, an attacker	
Service Pack 1 Update 3		·	1	1 '	the affected products are not	could have more understanding of	
		·	AV:L/AC:H/PR:H/UI:N/S:			the network and move laterally	EAVESDROPPING
Siemens SIMATIC WinAC RTX F	CVE-2016-	https://nvd.nist.	U/C:H/I: H/A:H	HIGH;HIGH;HIG	("C:\Program Files*" or the localized	inside the network, therefore	LATERAL MOVEMENT /
2010 Service Pack 2	7165	gov/vuln/detail/CVE-2016-7165	6,4 MEDIUM	Н	equivalent).	infecting other systems	PRIVILEGE ESCALATION
				/	1		
Siemens ETA4 Firmware 07 and				/	1		
11.0	A = -7	<i>A</i>		/	1		
Siemens SICAM TM; TM 1703	4	4		/	1		
Siemens SICAM AK ; AK 3	4	4		/	1		
Siemens SICAM BC; BC 1703		4			Specially crafted packets sent to		
Siemens SICAM AK Siemens		4			Port 2404/TCP could cause the		
SICAM AK 3 Siemens SICAM BC	A = -7	<i>A</i>			affected device to go into defect		
Siemens SICAM BC 1703		4	AV:N/AC:L/PR:N/UI:N/S:		mode. A cold start might be required		
	CVE-2016-	https://nvd.nist.			to recover the system, a Denial-of-		
SICAM TM 1703	7987	gov/vuln/detail/CVE-2016-7987	7,5 HIGH	Н	Service Vulnerability	a Denial of Service of the application	DENIAL OF SERVICE
•			1	1 '	1	an authenticated local attacker with	
•	1	·	1	1 '	Credentials Management Errors -	certain privileges could possibly	
Siemens SICAM PAS (Power	CVE-2016-	https://nvd.nist.	AV:L/AC:L/PR:L/UI:N/S:U/	HIGH;HIGH;HIG	Storing Passwords in a Recoverable	reconstruct the passwords of users	LATERAL MOVEMENT /
Automation System)	8566	gov/vuln/detail/CVE-2016-8566	C:H/I: H/A:H	н	Format	for accessing the database.	PRIVILEGE ESCALATION
				/	Use of Hard-coded Credentials -	Attackers might gain privileged	
Siemens SICAM PAS (Power	CVE-2016-	https://nvd.nist.	AV:N/AC:L/PR:N/UI:N/S:U				FALSE DATA INJECTION
,	8567				•		EAVESDROPPING
, ,		1			,		
		·	AVAMA OU /DDAN/ULAN/O		Exposure of Sensitive Information to	1	
ONATIO 07 000 ODLI	27.75 2040	1 ,	AV:N/AC:L/PR:N/UI:N/S:		an Unauthorized Actor - The	a de la configuração	
	CVE-2016-	https://nvd.nist.			=	Could get access to conficential	
	8672	gov/vuln/detail/CVE-2016-8672	153 MEDIUM	е	cookies without the "secure" flag	information	EAVESDROPPING

						could allow remote attackers to	
						perform actions with the permissions	
						of an authenticated user, provided	
			AV:N/AC:L/PR:N/UI:R/S:			the targeted user has an active	
Siemens SIMATIC S7 300 CPU	CVE-2016-	https://nvd.nist.	U/C:H/I: H/A:H	HIGH;HIGH;HIG		session and is induced to trigger the	
Siemens SIMATIC S7 400 CPU	8673	gov/vuln/detail/CVE-2016-8673	8,8 HIGH	Н	Cross-Site Request Forgery (CSRF)	malicious request	COMMAND INJECTION
						a culd all aux a warranta atta alcanta	
						could allow a remote attacker to upload, download, or delete files in	
						certain parts of the file system by	
Siemens SICAM PAS (Power	CVE-2016-	https://nvd.nist.	AV:N/AC:L/PR:N/UI:N/S:U	1 0001 0001 0		sending specially crafted packets to	EALSE DATA INTECTION
, ,	9156	gov/vuln/detail/CVE-2016-9156		W	Improper Access Control	port 19235/TCP	EAVESDROPPING
Automation System)	9130	gov/vum/detail/CVE-2016-9156	/C.L/I. L/A.L	VV	Improper Access Control	poil 19233/TCP	EAVESDROPPING
						could allow a remote attacker to	
						cause a Denial of Service condition	
						and potentially lead to	
						unauthenticated remote code	
`	CVE-2016-	https://nvd.nist.	AV:N/AC:L/PR:N/UI:N/S:U	HIGH;HIGH;HIG		execution by sending specially	COMMAND INJECTION
Automation System)	9157	gov/vuln/detail/CVE-2016-9157	/C:H/I: H/A:H	Н	Improper Input Validation	crafted packets to port 19234/TCP	DENIAL OF SERVICE
						By sending specially crafted	
						packets to the OPC Discovery	
						Server at port 4840/tcp, an attacker	
		https://nvd.nist.	AV:N/AC:L/PR:N/UI:N/S:			might cause the system to access	
	CVE-2017-	gov/vuln/detail/CVE-2017-	U/C:L/I: N/A:H	LOW;none;HIG		various resources chosen by the	
Siemens WinCC 7.4	12069	12069	8,2 HIGH	н	Entity Reference	attacker.	DENIAL OF SERVICE
						Specially crafted PROFINET DCP	
						broadcast packets could cause a	
						denial of service condition of	
						affected products on a local Ethernet	
			AV:A/AC:L/PR:N/UI:N/S:			segment (Layer 2). Human	
,	CVE-2017-	https://nvd.nist.	U/C:N/I: N/A:H	none;none;HIG		interaction is required to recover the	55,044, 65,655,065
W. PN	2680	gov/vuln/detail/CVE-2017-2680	6,5 MEDIUM	Н	Uncontrolled Resource Consumption	systems	DENIAL OF SERVICE
Siemens SIMATIC S7-1500							
Software Controller							
			AV:A/AC:L/PR:N/UI:N/S:				
Siemens SINAMICS G120 (C/P/D)	01/5 0047	to the continue of the first	U/C:N/I: N/A:H	none;none;HIG			
` '	CVE-2017-	https://nvd.nist.	U/C:N/I: N/A:H	none,none,nig			

Siemens SIMATIC WinCC Flexible 2008 Siemens SIMATIC WinCC (TIA Portal) 13.0						Specially crafted PROFINET DCP broadcast packets sent to the affected products on a local Ethemet segment (Layer 2) could cause a	
			AV:A/AC:L/PR:N/UI:N/S:			Denial-of-Service condition of some	
Siemens SIMATIC WinAC RTX F	CVE-2017-	https://nvd.nist.	U/C:N/I: N/A:H	none;none;HIG		services. The services require	
2010 Service Pack 2	6865	gov/vuln/detail/CVE-2017-6865	6,5 MEDIUM	Н	Improper Input Validation	manual restart to recover.	DENIAL OF SERVICE
			AV:N/AC:L/PR:L/UI:N/S:			Could allow a low privilege user to	
Siemens XHQ Server 4.7.1.2;	CVE-2017-	https://nvd.nist.	U/C:H/I: N/A:N	HIGH;none;non	Improper Access Control	gain reading access compromising	
5.0.0.1	6866	gov/vuln/detail/CVE-2017-6866	6,5 MEDIUM	е	vulnerability	this way the confidentiality	EAVESDROPPING
	ļ ,					could allow an authenticated, remote	
						attacker who is member of the	
						"administrators" group to crash	
			AV:N/AC:L/PR:H/UI:N/S:			services by sending specially	
Siemens SIMATIC WinCC 7.4	CVE-2017-	https://nvd.nist.	U/C:N/I: N/A:H	none;none;HIG		crafted messages to the DCOM	
Service Pack 1 Update 3	6867	gov/vuln/detail/CVE-2017-6867	4,9 MEDIUM	Н	Improper Input Validation	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;HIG H	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;HIG	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	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;HIG	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
1 01101/ 10.0	11707	11777	0,0111011	J	aciaan nistanation of the Coltai	umorom user.	I THE LOCALATION

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

	•	•	Ī		-	Ī	i i
						An attacker with local access to the	
						engineering system or in a privileged	
						network position and able to obtain	
			AV:N/AC:H/PR:L/UI:N/S:			certain network traffic could possibly	
	CVE-2018-	https://nvd.nist.	U/C:H/I: N/A:N	HIGH;none;non		reconstruct access authorization	LATERAL MOVEMENT /
SIPROTEC	4839	gov/vuln/detail/CVE-2018-4839	5,3 MEDIUM	a lioi i,none,non	Inadequate Encryption Strength	passwords.	PRIVILEGE ESCALATION
SII KOILO	4039	gov/vum/detail/CVL-2010-4033	3,3 NILDION	С	madequate Encryption Stierigth	passwolus.	TRIVILLOL LOCALATION
						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	
					A service of the affected products	application on the host. In order to	
					listening on all of the host's network	execute arbitrary code with Microsoft	
					interfaces on either port 4884/TCP,	Windows user permissions, an	
					5885/TCP, or port 5886/TCP could	attacker must be able to plant the	
					allow an attacker to either exfiltrate	code in advance on the host by other	
Siemens SICAM SCC			AV:L/AC:L/PR:N/UI:R/S:		limited data from the system or to	means. The vulnerability has limited	
	CVE-2018-	https://nvd.nist.	U/C:H/I: H/A:H	HIGH;HIGH;HIG	execute code with Microsoft	impact to confidentiality and integrity	COMMAND INJECTION
Siemens SICAM PQ ANALYZER	4858	gov/vuln/detail/CVE-2018-4858	7,8 HIGH	Н	Windows user permissions	of the affected system	EAVESDROPPING
Siemens SIMATIC WinCC (TIA							
Portal) 13.0							
Siemens SIMATIC WinCC 7.4						An attacker with access to the	
Service Pack 1 Update 3		,	AN / AN / A O I / IDD I / III AN / O			project file could run arbitrary system	
	0) (5 0040	https://nvd.nist.	AV:N/AC:L/PR:L/UI:N/S:		Improper Neutralization of Special	commands with the privileges of the	
Siemens SIMATIC WinCC Runtime		gov/vuln/detail/CVE-2019-	U/C:H/I: H/A:H	HIGH;HIGH;HIG	Elements used in an SQL Command	local database server, and therefore	COMMAND INJECTION
Professional 13 Special Pack 1	10916	<u>10916</u>	8,8 HIGH	п	('SQL Injection')	it takes a bit hit in CIA	FALSE DATA INJECTION
Siemens SIMATIC WinCC (TIA							
Portal) 13.0						An attacker with local access to the	
Siemens SIMATIC WinCC 7.4						project file could cause a Denial-of-	
Service Pack 1 Update 3						Service condition on the affected	
		https://nvd.nist.	AV:L/AC:L/PR:L/UI:N/S:U			product while the project file is	
Siemens SIMATIC WinCC Runtime	CVE-2019-	gov/vuln/detail/CVE-2019-	/C:N/I: N/A:H	none:none:HIG	Improper Handling of Exceptional	loaded. Successful exploitation	
Professional 13 Special Pack 1	10917	10917	5,5 MEDIUM	Н	Conditions	requires access to the project file	DENIAL OF SERVICE

	ı	T	T	T			1
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;HIG H	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;HIG H	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/CVF-2019- 10923	AV:N/AC:L/PR:N/UI:N/S: U/C:N/I: N/A:H 7,5 HIGH	none;none;HIG H	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;non e	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/CVF-2019- 10930	AV:N/AC:L/PR:N/UI:N/S: U/C:N/I: H/A:N 7,5 HIGH	none;HIGH;non e	Unrestricted Upload of File with Dangerous Type	system.	FALSE DATA INJECTION EAVESDROPPING
SIPROTEC	CVE-2019- 10931	https://nvd.nist. gov/vuln/detail/CVF-2019- 10931	AV:N/AC:L/PR:N/UI:N/S: U/C:N/I: N/A:H 7,5 HIGH	none;none;HIG H	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	CVE-2019-	gov/vuln/detail/CVE-2019-			handle large amounts of specially	could allow an unauthenticated remote attacker to trigger a denial of	
Siemens SINAMICS G120	10936	<u>10936</u>	7,5 HIGH	H	crafted UDP packets.	service condition.	DENIAL OF SERVICE
SIPROTEC	CVE-2019- 10938	gov/vuln/detail/CVE-2019-		HIGH;HIGH;HIG H		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	gov/vuln/detail/CVE-2019-	AV:N/AC:L/PR:N/UI:N/S: U/C:N/I: H/A:N 7,5 HIGH	none;HIGH;non	Insufficient Verification of Data Authenticity - The vulnerability could impact the perceived integrity of the	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	t
Siemens S7-1200 CPU 1211C; 1212C 1212f 1214C 1214fc 1215C 1215fc 1217c	CVE-2019- 13940	gov/vuln/detail/CVE-2019-		none;none;HIG H		an attacker could send specially crafted HTTP requests to ports 80/tcp and 443/tcp and lead to a DoS of the web server	
Esri ArcGIS Enterprise Esri ArcGIS Enterprise 10.6.1	CVE-2019- 16193	gov/vuln/detail/CVE-2019-	AV:N/AC:L/PR:L/UI:R/S: C/C:L/I: L/A:N 5,4 MEDIUM	LOW;LOW;non	During Web Page Generation ('Cross-	, , ,	COMMAND INJECTION
SIPROTEC	CVE-2019- 19279	gov/vuln/detail/CVE-2019-		none;none;HIG H		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
	CVE-2019- 6568	https://nvd.nist.		none;none;HIG H		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	CVE-2019-	https://nvd.nist.	AV:N/AC:L/PR:N/UI:N/S: U/C:H/I: H/A:N	HIGH;HIGH;non	Use of Hard-coded Credentials - The affected device offered SNMP read and write capacities with a publicly	An attacker could use the vulnerability to compromise confidentiality and integrity of the	FALSE DATA INJECTION
Portal) 13.0	6572	gov/vuln/detail/CVE-2019-6572	9,1 CRITICAL	e	know hardcoded community string Improper Handling of Exceptional Conditions	affected system. Could allow an unauthenticated	EAVESDROPPING
			AV:N/AC:L/PR:N/UI:N/S:		- Specially crafted network packets	remote attacker to cause a denial of	
Siemens SIMATIC S7-1500	CVE-2019-	https://nvd.nist.	U/C:N/I: N/A:H	none;none;HIG	sent to affected devices on port	service condition of the OPC	DENIAL OF CEDVICE
Software Controller	6575	gov/vuln/detail/CVE-2019-6575	7,5 HIGH	Н	4840/tcp	communication or crash the device.	DENIAL OF SERVICE
Siemens SIMATIC WinCC (TIA Portal) 13.0	CVE-2019- 6576	https://nvd.nist.	AV:N/AC:L/PR:N/UI:N/S: U/C:H/I: N/A:N 7,5 HIGH	HIGH;none;non	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
			,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,				
			AV:N/AC:L/PR:L/UI:R/S:		Improper Neutralization of Input	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	
Siemens SIMATIC WinCC (TIA	CVE-2019-	https://nvd.nist.	C/C:L/I: L/A:N	LOW;LOW;non	During Web Page Generation ('Cross-	confidentiality and the integrity of the	
Portal) 13.0	6577	gov/vuln/detail/CVE-2019-6577	5,4 MEDIUM	е	site Scripting')	affected system.	EAVESDROPPING

						By performing a flooding attack	
						against the web server, an attacker	
Siemens SICAM MMU Siemens		https://nvd.nist.	AV:N/AC:L/PR:N/UI:N/S:			might be able to gain read access to	
SICAM SGU Siemens SICAM T	CVE-2020-	gov/vuln/detail/CVE-2020-	U/C:H/I: N/A:N	HIGH;none;non		the device's memory, possibly	
Siemens SICAM SGU Firmware	10037	10037	7,5 HIGH	е	Out-of-bounds Read	revealing confidential information	EAVESDROPPING
						An attacker with access to the	
Siemens SICAM MMU Siemens		https://nvd.nist.	AV:N/AC:L/PR:N/UI:N/S:			device's web server might be able to	
SICAM SGU Siemens SICAM T	CVE-2020-	gov/vuln/detail/CVE-2020-	U/C:H/I: H/A:H	HIGH:HIGH:HIG	Missing Authentication for Critical	execute administrative commands	
Siemens SICAM SGU Firmware	10038	10038	9,8 CRITICAL		Function	without authentication.	COMMAND INJECTION
			-,-				
						An attacker in a privileged network	
						position between a legitimate user	
						and the web server might be able to	
Siemens SICAM MMU Siemens		https://nvd.nist.	AV:N/AC:H/PR:N/UI:N/S:			conduct a Man-in-the-middle attack	
SICAM SGU Siemens SICAM T	CVE-2020-	gov/vuln/detail/CVE-2020-	U/C:H/I: H/A:H		Missing Encryption of Sensitive	and gain read and write access to	FALSE DATA INJECTION
Siemens SICAM SGU Firmware	10039	10039	8,1 HIGH	Н	Data	the transmitted data	EAVESDROPPING
Siemens SICAM MMU Siemens		https://nvd.nist.	AV:L/AC:L/PR:L/UI:N/S:U			An attacker with local access to the	
SICAM SGU Siemens SICAM T	CVE-2020-	gov/vuln/detail/CVE-2020-	/C:H/I: N/A:N	HIGH;none;non	Use of Password Hash With	device might be able to retrieve	
Siemens SICAM SGU Firmware	10040	10040	5,5 MEDIUM	е	Insufficient Computational Effort	some passwords in clear text.	EAVESDROPPING
Siemens SICAM MMU Siemens		https://nvd.nist.	AV:N/AC:L/PR:N/UI:R/S:		Improper Neutralization of Input		
SICAM SGU Siemens SICAM T	CVE-2020-	gov/vuln/detail/CVE-2020-	C/C:L/I: L/A:N	LOW;LOW;non	During Web Page Generation ('Cross-	An attacker might be able to take	LATERAL MOVEMENT /
Siemens SICAM SGU Firmware	10041	10041	6,1 MEDIUM	е	site Scripting')	over a session of a legitimate user.	PRIVILEGE ESCALATION
						might enable an attacker with	
Siemens SICAM MMU Siemens		https://nvd.nist.	AV:N/AC:L/PR:N/UI:N/S:			access to the web application to	
SICAM SGU Siemens SICAM T	CVE-2020-	gov/vuln/detail/CVE-2020-	U/C:H/I: H/A:H	HIGH:HIGH:HIG	Buffer Copy without Checking Size	execute arbitrary code over the	COMMAND INJECTION
Siemens SICAM SGU Firmware	10042	10042	9,8 CRITICAL	Н	of Input ('Classic Buffer Overflow')	network.	DENIAL OF SERVICE
			.,.		,		
Oi		latter a effect of order	AVANIA O.L /DD-N/ULD/O.		Income and New York in the second	could allow Cross-Site Scripting	
Siemens SICAM MMU Siemens	0)/5 0000	https://nvd.nist.	AV:N/AC:L/PR:N/UI:R/S:	1 0/4/-1 0/4/	Improper Neutralization of Input	(XSS) attacks if unsuspecting users	
SICAM SGU Siemens SICAM T	CVE-2020-		C/C:L/I: L/A:N	LOW;LOW;non	During Web Page Generation ('Cross-	are tricked into accessing a	OTHER
Siemens SICAM SGU Firmware	10043	10043	6,1 MEDIUM	е	site Scripting')	malicious link.	OTHER
						An attacker with access to the	
Siemens SICAM MMU Siemens		https://nvd.nist.	AV:N/AC:L/PR:N/UI:N/S:			network could be able to install	
SICAM SGU Siemens SICAM T	CVE-2020-	gov/vuln/detail/CVE-2020-	U/C:N/I: H/A:N	none;HIGH;non	Missing Authentication for Critical	specially crafted firmware to the	FALSE DATA INJECTION
Siemens SICAM SGU Firmware	10044	10044	7,5 HIGH	е	Function	device.	PERSISTENCE
						An error in the challenge- response	
						procedure could allow an attacker to	
Siemens SICAM MMU Siemens		https://nvd.nist.	AV:N/AC:L/PR:N/UI:R/S:			replay authentication traffic and gain	
SICAM SGU Siemens SICAM T	CVE-2020-	gov/vuln/detail/CVE-2020-	U/C:H/I: H/A:H	HIGH;HIGH;HIG	Authentication Bypass by Capture-	access to protected areas of the web	
Siemens SICAM SGU Firmware	10045	10045	8,8 HIGH	Н	replay	application.	ACCESS

		1				Γ	
						An attacker could bypass the	
						password protection set on protected	
		https://nvd.nist.	AV:L/AC:L/PR:L/UI:N/S:U			files, thus being granted access to	
Siemens SIMATIC WinCC 7.4	CVE-2020-	gov/vuln/detail/CVE-2020-	/C:H/I: N/A:N	HIGH;none;non	Improper Authentication - insecure	the protected content, circumventing	
Service Pack 1 Update 3	10048	10048	5,5 MEDIUM	е	password verification process	authentication.	EAVESDROPPING
					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,	This Cross-Site-Scripting (XSS)	
		https://nvd.nist.	AV:N/AC:L/PR:N/UI:R/S:		these log messages might be	vulnerability might compromize the	
	CVE-2020-	gov/vuln/detail/CVE-2020-	C/C:H/I: H/A:H	HIGH;HIGH;HIG	interpreted and executed as code by	confidentiality, integrity and	
Siemens SICAM A8000	15781	15781	9,6 CRITICAL	Н	the web application.	availability of the web application.	OTHER
						could allow a remote attacker to	
		https://nvd.nist.	AV:N/AC:L/PR:N/UI:N/S:			trigger a denial-of-service condition	
Siemens SIMATIC ET 200SP	CVE-2020-	gov/vuln/detail/CVE-2020-	U/C:N/I: N/A:H	none;none;HIG		00	
Open Controller	15796	15796	7.5 HIGH	none,none,nig	I lead with Everation	by sending a specially crafted HTTP	DENIAL OF SERVICE
Open Controller	15796			П	Uncaught Exception	request	DENIAL OF SERVICE
		https://nvd.nist.	AV:L/AC:L/PR:L/UI:N/S:C			could allow an attacker to disclose	
Siemens SIMATIC ET 200SP	CVE-2020-	gov/vuln/detail/CVE-2020-	/C:H/I: N/A:N	HIGH;none;non	Domain-bypass transient execution	confidential information if they are	
Open Controller	24513	<u>24513</u>	6,6 MEDIUM	е	vulnerability	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		https://nvd.nist.	AV:N/AC:L/PR:N/UI:N/S:				
Esri ArcGIS Server 10.6.1 on X64	CVE-2020-	gov/vuln/detail/CVE-2020-	U/C:H/I: H/A:H	HIGH;HIGH;HIG		an attacker could retrieve senstivie	
Esri ArcGIS Server 10.7.1 on X64	35712	35712	9,8 CRITICAL	Н	SSRF	information from the server	EAVESDROPPING
Siemens SIMATIC WinCC Runtime					A common component used by the		
					· · · · · · · · · · · · · · · · · · ·		
Professional 13 Special Pack 1			AV.1. /A C.1. /DD.1.1/11/AV/C.		affected applications regularly calls	This sould allow a local attackers	
Siemens	0)/5 0000	latter and training	AV:L/AC:L/PR:H/UI:N/S:		a helper binary with SYSTEM	This could allow a local attacker to	
SIMATIC S7-1500	CVE-2020-	https://nvd.nist.	U/C:H/I: H/A:H		privileges while the call path is not	execute arbitrary code with SYTEM	
Software Controller	7580	gov/vuln/detail/CVE-2020-7580	6,7 MEDIUM	Н	quoted.	privileges.	COMMAND INJECTION

1		1	ı		T	ı	1
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;HIG H	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;HIG H	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		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			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 ———————————————————————————————————	CVE-2021- 29096	https://nvd.nist. gov/vuln/detail/CVE-2021- 29096		нісн;нісн;ніс н	use-after-free vulnerability when parsing a specially crafted file	allow an <u>unauthenticated</u> 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 10.1 ESRI ArcGIS 10.8.1 ESRI ArcGIS Desktop ESRI ArcGIS Desktop 10.8.1 ———————————————————————————————————	CVE-2021-	https://nvd.nist. gov/vuln/detail/CVE-2021-	AV:L/AC:L/PR:N/UI:R/S: U/C:H/I: H/A:H		Multiple buffer overflow vulnerabilities when parsing a	allow an unauthenticated attacker to achieve arbitrary code execution in	
2.7;	29097	29097		ніон,піон,піо Н	specially crafted file	the context of the current user.	COMMAND INJECTION

	I	T	T	r			
ESRI ArcGIS ESRI ArcGIS 9.0							
ESRI ArcGIS 10.0.2.3200							
ESRI ArcGIS 10.0.2.3200							
ESRI AreGIS 10.1							
ESRI ArcGIS 10.8.1							
ESRI ArcGIS Desktop							
ESRI ArcGIS Desktop 10.8.1		latter a discord or in t	A) (-1 /A O-1 /DD-N/UI-D/O-		Maritin I a control d'alle and a control		
	0) /5 0004	https://nvd.nist.	AV:L/AC:L/PR:N/UI:R/S:		Multiple uninitialized pointer	allow an unauthenticated attacker to	
Esri ArcGIS Pro 2.6; 2.6.5;	CVE-2021-	gov/vuln/detail/CVE-2021-	U/C:H/I: H/A:H		vulnerabilities when parsing a	achieve arbitrary code execution in	COMMAND IN FOTION
2.7;	29098	<u>29098</u>	7,8 HIGH	H	specially crafted file	the context of the current user.	COMMAND INJECTION
Esri ArcGIS Server							
Esri ArcGIS Server 10.2.2 Esri							
ArcGIS Server 10.2.2 Esti							
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		https://nvd.nist.	AV:N/AC:L/PR:N/UI:N/S:		Improper Neutralization of Special		
Esri ArcGIS Server 10.0.1 on X64	CVE-2021-	gov/vuln/detail/CVE-2021-	U/C:L/I: N/A:N	LOW;none;non	Elements used in an SQL Command	Specially arafted web requests can	
Esri ArcGIS Server 10.7.1 on X64	29099	29099	5,3 MEDIUM	COVV, HOHE, HOH	('SQL Injection')	expose information	EAVESDROPPING
ESII AICGIS Seiver 10.6.1 011 X04	29099	<u>29099</u>	5,3 WEDIOW	е	(SQL IIIJection)	expose information	EAVESDROPFING
						An attacker could exploit this	
Esri ArcGIS Earth 1.7.0; 1.8.0;						vulnerability to gain arbitrary code	
1.9.0;						execution under security context of	
1.10.0;		https://nvd.nist.	AV:L/AC:L/PR:N/UI:R/S:			the user running ArcGIS Earth by	
1.10.1;	CVE-2021-	gov/vuln/detail/CVE-2021-	U/C:H/I: H/A:H	HIGH;HIGH;HIG		inducing the user to upload a crafted	COMMAND INJECTION
1.11.0;	29100	29100	7,8 HIGH	Н	A path traversal vulnerability	file to an affected system	FALSE DATA INJECTION
						could allow an unauthenticated,	
		https://nvd.nist.	AV:N/AC:L/PR:N/UI:N/S:			remote attacker to perform directory	
ArcGIS GeoEvent Server ArcGIS	CVE-2021-	gov/vuln/detail/CVE-2021-	U/C:H/I: N/A:N	HIGH;none;non	has a read-only directory path	traversal attacks and read arbitrary	
GeoEvent Server 10.8.1	29101	29101	7,5 HIGH	е	traversal vulnerability	files on the system	EAVESDROPPING
					,		
			ĺ			may allow a <u>remote.</u>	
E : A 010 0			ĺ			unauthenticated attacker to forge	
Esri ArcGIS Server on X64		,	A.V. A.V.A.O. L. //E.D			GET requests to arbitrary URLs from	
Esri ArcGIS Server 10.6.1 on X64	0.45 0004	https://nvd.nist.	AV:N/AC:L/PR:N/UI:N/S:			the system, potentially leading to	
Esri ArcGIS Server 10.7.1 on X64	CVE-2021-	gov/vuln/detail/CVE-2021-	U/C:H/I: H/A:N	HIGH;HIGH;non	0 0 0 0	network enumeration or facilitating	E 4) /EODDODO:::0
Esri ArcGIS Server 10.8.1 on X64	29102	29102	9,1 CRITICAL	е	Server-Side Request Forgery (SSRF)	other attacks	EAVESDROPPING

			_				
	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;non	Improper Neutralization of Input During Web Page Generation ('Cross- site Scripting') - reflected Cross Site	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;non	stored Cross Site Scripting (XXS)	allow a <u>remote unauthenticated</u> 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;non		may allow a <u>remote authenticated</u> 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;non	Improper Neutralization of Input	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 ArcGlS Server 10.6.1 on X64	CVE-2021- 29107	https://nvd.nist. gov/vuln/detail/CVF-2021- 29107	AV:N/AC:L/PR:N/UI:R/S: C/C:L/I: L/A:N 6,1 MEDIUM	LOW;LOW;non	Improper Neutralization of Input	may allow a remote unauthenticated attacker to pass and store malicious strings in the ArcGIS Server Manager application.	FALSE DATA INJECTION
	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;HIG H	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;non	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;non	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;non e	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	CVE-2021-	https://nvd.nist. gov/vuln/detail/CVE-2021-	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	LOW;LOW;LO	Improper Neutralization of Special Elements used in an SQL Command	allows a <u>remote</u> , <u>unauthenticated</u> attacker to impact the confidentiality, integrity and availability of targeted services via	FALSE DATA INJECTION EAVESDROPPING
Esri ArcGIS Server 10.8.1 on X64 Esri ArcGIS Server 10.9.0 on X64	29114	29114	9,8 CRITICAL> NIST	W (LOW;LO	('SQL Injection')	availability of targeted services via specifically crafted queries	DENIAL OF SERVICE

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

	T		•				
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		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;HIG H	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;HIG H	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;non	Traversal') - When downloading files,	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		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

		ı					
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					Improper Input Validation Affected		
12 1215fc		https://nvd.nist.	AV:N/AC:L/PR:N/UI:N/S:		devices don't process correctly		
Siemens SIMATIC S7-1200 CPU	CVE-2021-	gov/vuln/detail/CVE-2021-	U/C:N/I: N/A:H	none;none;HIG	certain special crafted packets sent	could allow an attacker to cause a	
12 1217C	40365	40365	7,5 HIGH	Н	to port 102/tcp	denial of service in the device	DENIAL OF SERVICE
						An improper input validation	
		https://nvd.nist.	AV:N/AC:L/PR:N/UI:N/S:			vulnerability in the web server could	
	CVE-2021-	gov/vuln/detail/CVE-2021-	U/C:H/I: N/A:N	HIGH;none;non		allow an unauthenticated user to	
SIPROTEC	41769	41769	7.5 HIGH	n liGi i,rione,rion	Improper Input Validation	access device information.	EAVESDROPPING
SIFKOILG	41709		,	6	improper input vandation		LAVESDROFFING
		https://nvd.nist.	AV:L/AC:L/PR:L/UI:N/S:U			An attacker could achieve privilege	
	CVE-2021-	gov/vuln/detail/CVE-2021-	/C:H/I: H/A:H	HIGH;HIGH;HIG		escalation on the web server of	LATERAL MOVEMENT /
Siemens SIMATIC S7-1500 CPU	42029	<u>42029</u>	7,8 HIGH	Н	Improper Access Control	certain devices	PRIVILEGE ESCALATION
Siemens (SICAM Q100) 7KG9501-							
0AA01-0AA1						could allow a remote attacker with	
		https://nvd.nist.	AV:N/AC:L/PR:H/UI:N/S:			engineer or admin priviliges to	
Siemens (SICAM Q100) 7KG9501-	CVE-2021-	gov/vuln/detail/CVE-2021-	U/C:H/I: H/A:H	HIGH;HIGH;HIG		potentially perform remote code	
0AA31-2AA1	44165	44165	7,2 HIGH	н	Stack-based Buffer Overflow	execution.	COMMAND INJECTION
		_					
Siemens EnergyIP 8.5							
Siemens EnergyIP 8.6							
Siemens EnergyIP 8.7						An attacker who can control log	
Siemens EnergyIP 9.0						messages or log message	
Siemens					log messages, and parameters do	parameters can execute arbitrary	
SIGUARD DSA 4.2		https://nvd.nist.	AV:N/AC:L/PR:N/UI:N/S:		not protect against attacker	code loaded from LDAP servers	
Siemens SIGUARD DSA 4.3	CVE-2021-	gov/vuln/detail/CVE-2021-	C/C:H/I: H/A:H	HIGH;HIGH;HIG	controlled LDAP and other JNDI	when message lookup substitution	
Siemens SIGUARD DSA 4.4	44228	44228	10,0 CRITICAL	Н	related endpoints	is enabled.	COMMAND INJECTION

							I
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							ļ
12 1214C							
Siemens SIMATIC S7-1200 CPU							
12 1214fc							
Siemens SIMATIC S7-1200 CPU							
12 1215C							
Siemens SIMATIC S7-1200 CPU					Improper Input Validation Affected		
12 1215fc		https://nvd.nist.	AV:N/AC:L/PR:N/UI:N/S:		devices don't process correctly		
Siemens SIMATIC S7-1200 CPU	CVE-2021-	gov/vuln/detail/CVE-2021-	U/C:N/I: N/A:H	none;none;HIG	certain special crafted packets sent	could allow an attacker to cause a	
12 1217C	44693	44693	7,5 HIGH	Н	to port 102/tcp	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					Improper Input Validation Affected		
		https://pvd.mist	ANAMA OLI /DDIAI/LUAN/OL		Improper Input Validation Affected		
12 1215fc	0)/5 0004	https://nvd.nist	AV:N/AC:L/PR:N/UI:N/S:		devices don't process correctly		
Siemens SIMATIC S7-1200 CPU	CVE-2021-	gov/vuln/detail/CVE-2021-	U/C:N/I: N/A:H		certain special crafted packets sent		DENIAL OF CEDVICE
12 1217C	44694	<u>44694</u>	7,5 HIGH	H	to port 102/tcp	denial of service in the device	DENIAL OF SERVICE

		1		1			
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					Impressor Impret Validation Affacts d		
Siemens SIMATIC S7-1200 CPU 12 1215fc		https://nvd.nist.	AV:N/AC:L/PR:N/UI:N/S:		Improper Input Validation Affected		
Siemens SIMATIC S7-1200 CPU	CVE-2021-		U/C:N/I: N/A:H		devices don't process correctly	could allow an attacker to cause a	
12 1217C	44695	gov/vuln/detail/CVE-2021- 44695	7,5 HIGH	none;none;HIG	certain special crafted packets sent		DENIAL OF SERVICE
12 12170	44090	44030	7,3 HIGH	11	to port 102/tcp	denial of service in the device	DEINIAL OF SERVICE
Siemens EnergyIP 8.5							
Siemens EnergyIP 8.6							
Siemens EnergyIP 8-7 -							
Siemens EnergyIP 9.0							
Siemens SIGUARD DSA 4.2		https://nvd.nist.	AV:N/AC:H/PR:N/UI:N/S:		Improper Neutralization of Special		
Siemens SIGUARD DSA 4.3	CVE-2021-	gov/vuln/detail/CVE-2021-	C/C:H/I: H/A:H	HIGH;HIGH;HIG	Elements used in an Expression		
Siemens SIGUARD DSA 4.4	45046	<u>45046</u>	9,0 CRITICAL	Н	Language Statement		FALSE DATA INJECTION
					Use of Hard-coded Credentials -		
		https://nvd.nist.	AV:N/AC:L/PR:L/UI:N/S:		Affected applications use a		
	CVE-2021-	gov/vuln/detail/CVE-2021-	U/C:H/I: N/A:N	HIGH;none;non	circumventable access control	This could allow an attacker to	
Siemens SICAM Toolbox II	45106	<u>45106</u>	6,5 MEDIUM	е	within a database service	access the database.	EAVESDROPPING
						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	
		https://py.d.pist	AVANIA CALIDDALIANO		Unavioted Coords Dath on Element	the legitimate process. Attackers	FALCE DATA INTECTION
	C)/E 2024	https://nvd.nist.	AV:N/AC:L/PR:L/UI:N/S:	noned BOLLER	Unquoted Search Path or Element -	might achieve persistence on the	FALSE DATA INJECTION
Sigmons CICAM DO ANALYZED	CVE-2021-	gov/vuln/detail/CVE-2021-	U/C:N/I: H/A:H	none;HIGH;HIG	A service is started by an unquoted	system ("backdoors") or cause a	DENIAL OF SERVICE
Siemens SICAM PQ ANALYZER	45460	<u>45460</u>	8,1 HIGH	П	registry entry	denial of service	PERSISTENCE
					Insecure Default Initialization of		
					Resource - a missing printer	This could allow an attacker to view	
		https://nvd.nist.	AV:L/AC:L/PR:L/UI:N/S:U		configuration on the host could allow	sensitive information, run tasks	
Siemens SIMATIC WinCC Runtime		gov/vuln/detail/CVE-2022-	/C:H/I: H/A:H	HIGH;HIGH;HIG	an authenticated attacker to escape	outside the intended scope and	
Professional 13 Special Pack 1	24287	<u>24287</u>	7,8 HIGH	Н	the WinCC Kiosk Mode.	therefore have an impact in the CIA	EAVESDROPPING

			I				
Siemens SIMATIC WinCC Runtime					Insecure Default Initialization of		
Professional 13 Special Pack 1					Resource - a missing printer	This could allow an attacker to view	
		https://nvd.nist.	AV:L/AC:L/PR:L/UI:N/S:U		configuration on the host could allow	sensitive information, run tasks	
Siemens SIMATIC WinCC 7.4	CVE-2022-	gov/vuln/detail/CVE-2022-	/C:H/I: H/A:H	HIGH:HIGH:HIG	an authenticated attacker to escape	outside the intended scope and	
Service Pack 1 Update 3	24287	24287	7.8 HIGH	Н	the WinCC Kiosk Mode.	therefore have an impact in the CIA	EAVESDROPPING
Colvide Lack Lepadie C	21207		7,0 111011		the Willes Ricck Mode.	and the control of th	L/WEODITON INTO
			AV:N/AC:L/PR:N/UI:N/S:		Uncontrolled Resource Consumption		
			U/C:N/I: N/A:L		- The PROFINET (PNIO) stack, when		
			5,3 MEDIUM>		integrated with the Intemiche IP	could allow an attacker to create a	
			SIEMENS		stack, improperly handles internal	denial of service condition for TCP	
		https://nvd.nist.	AV:N/AC:L/PR:N/UI:N/S:		resources for TCP segments where	services on affected devices by	
	CVE-2022-	gov/vuln/detail/CVE-2022-	U/C:N/I: N/A:H	none;none;LO	the minimum TCP-Header length is	sending specially crafted TCP	
Siemens SIMATIC S7-1500 CPU	25622	25622	7,5 HIGH> NIST	w	less than defined	segments.	DENIAL OF SERVICE
						This could allow an authenticated	
						attacker to set the device to a denial	
		https://nvd.nist.	AV:N/AC:L/PR:L/UI:N/S:		Improper Input Validation - Affected	of service state or to control the	
SICAM P850	CVE-2022-	gov/vuln/detail/CVE-2022-	U/C:H/I: H/A:H	HIGH;HIGH;HIG	devices do not properly validate	program counter and, thus, execute	COMMAND INJECTION
SICAM P855	29872	29872	8,8 HIGH	Н	parameters of POST requests	arbitrary code on the device.	DENIAL OF SERVICE
					Improper Neutralization of	Could allow an unauthenticated	
					Parameter/Argument Delimiters -	attacker to set the device to a denial	
		https://nvd.nist.	AV:N/AC:L/PR:N/UI:N/S:		Affected devices do not properly	of service state or to control the	
SICAM P850	CVE-2022-	gov/vuln/detail/CVE-2022-	U/C:H/I: H/A:H	nicn·nicn·nic	validate parameters of certain GET	program counter and, thus, execute	COMMAND INJECTION
SICAM P855	29873	29873	9.8 CRITICAL	LI IIGI I,I IIGI I,I IIG	and POST requests.	arbitrary code on the device.	DENIAL OF SERVICE
SICAM P655	29013	29013	9,0 CRITICAL	П	and POST requests.	arbitrary code on the device.	DENIAL OF SERVICE
					Cleartext Transmission of Sensitive		
					Information - Affected devices do	This could allow an unauthenticated	
		https://nvd.nist.	AV:N/AC:L/PR:N/UI:N/S:		not encrypt web traffic with clients	attacker to capture the traffic and	
SICAM P850	CVE-2022-	gov/vuln/detail/CVE-2022-	U/C:H/I: N/A:N	HIGH;none;non	but communicate in cleartext via	interfere with the functionality of the	
SICAM P855	29874	29874	7,5 HIGH	е	нттр	device.	EAVESDROPPING
					Improper Neutralization of Innut	The provided engineers is directly	
					Improper Neutralization of Input	The provided argument is directly reflected in the web server response.	
		https://prod.mist	AV/AN/A C.L /DD:AL/LU:D/O		During Web Page Generation ('Cross-	· '	
OLOAM POSO	0)/5 0000	https://nvd.nist	AV:N/AC:L/PR:N/UI:R/S:		site Scripting') - Affected devices do	This could allow an unauthenticated	
SICAM P850	CVE-2022-	gov/vuln/detail/CVE-2022-	C/C:L/I: L/A:N	LOW;none;non	not properly handle the input of a	attacker to perform reflected XSS	OTHER
SICAM P855	29876	<u>29876</u>	6,1 MEDIUM	е	GET request parameter.	attacks.	OTHER
					Missing Authentication for Critical		
		https://nvd.nist.	AV:N/AC:L/PR:N/UI:N/S:		Function - Affected devices allow	This could allow an attacker to	
SICAM P850	CVE-2022-	gov/vuln/detail/CVE-2022-	U/C:L/I: L/A:N	LOW;LOW;non	unauthenticated access to the web	extract internal configuration details	
SICAM P855	29877	<u>29877</u>	6,5 MEDIUM	е	interface configuration area.	or to reconfigure network settings.	EAVESDROPPING

	•		1				
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;HIG H	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;non	Missing Authentication for Critical Function - The web based management interface of affected devices does not employ special	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;non	Improper Neutralization of Input During Web Page Generation ('Crosssite 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;non	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;non	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;non	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

1		T	T	1			1
Siemens SICAM GridEdge							
Essential ARM Edition Siemens							
SICAM GridEdge Essential GDS							
ARM Edition Siemens SICAM					Origin Validation Error - does not	In case an attacker tricks a	
GridEdge Essential GDS Intel		https://nvd.nist.	AV:N/AC:L/PR:N/UI:R/S:		apply cross-origin resource sharing	legitimate user into accessing a	
Edition Siemens SICAM GridEdge	CVE-2022-	gov/vuln/detail/CVE-2022-	U/C:N/I: H/A:N	none;HIGH;non	(CORS) restrictions for critical	special resource a malicious request	
Essential Intel Edition	30228	30228	6,5 MEDIUM	е	operations	could be executed.	OTHER
0: 0.0444.0 : 15.1							
Siemens SICAM GridEdge							
Essential ARM Edition Siemens							
SICAM GridEdge Essential GDS							
ARM Edition Siemens SICAM						This could allow an unauthenticated	
GridEdge Essential GDS Intel		https://nvd.nist.	AV:N/AC:L/PR:N/UI:N/S:			attacker to change data of an user,	
Edition Siemens SICAM GridEdge	CVE-2022-	gov/vuln/detail/CVE-2022-	U/C:N/I: L/A:N	none;LOW;non	Missing Authentication for Critical	such as credentials, in case that	
Essential Intel Edition	30229	30229	5,3 MEDIUM	е	Function	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		https://nvd.nist.	AV:N/AC:L/PR:N/UI:N/S:			This could allow an unauthenticated	
Edition Siemens SICAM GridEdge	CVE-2022-	gov/vuln/detail/CVE-2022-	U/C:H/I: H/A:H	HIGH:HIGH:HIG	Missing Authentication for Critical	attacker to create a new user with	
Essential Intel Edition	30230	30230	9.8 CRITICAL	Н	Function	administrative permissions.	ACCESS
Siemens SICAM GridEdge							
Essential ARM Edition Siemens							
SICAM GridEdge Essential GDS					Transmission of Private Resources		
ARM Edition Siemens SICAM					into a New Sphere ('Resource Leak') -		
GridEdge Essential GDS Intel		https://nvd.nist.	AV:N/AC:L/PR:L/UI:N/S:		The affected software discloses	This could allow an authenticated	
Edition Siemens SICAM GridEdge	CVE-2022-	gov/vuln/detail/CVE-2022-	U/C:L/I: N/A:N	LOW;none;non	password hashes of other users	user to retrieve another users	
Essential Intel Edition	30231	<u>30231</u>	4,3 MEDIUM	е	upon request	password hash.	EAVESDROPPING

			Ī	I	T		T
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			AV:N/AC:L/PR:N/UI:R/S:				
12 1215fc			U/C:H/I: N/A:N				
Siemens SIMATIC S7-1200 CPU			6,5 MEDIUM>		Cross-Site Request Forgery (CSRF) -		
12 1217C			SIEMENS		login endpoint	could allow authenticated remote	
Siemens		https://nvd.nist.	AV:N/AC:L/PR:L/UI:R/S:		/FormLogin in affected web services	attackers to track the activities of	
SIMATIC S7-1500	CVE-2022-	gov/vuln/detail/CVE-2022-	U/C:L/I: N/A:N	LOW;none;non	does not apply proper origin	other users via a login cross-site	
Software Controller	30694	30694	3,5 LOW> NIST	е	checking	request forgery attack	EAVESDROPPING
Siemens SICAM GridEdge					Exposure of Resource to Wrong	Attackers with access to the	
Essential ARM		https://nvd.nist.	AV:L/AC:L/PR:L/UI:N/S:U		Sphere - Affected software uses an	filesystem of the host on which	
Siemens SICAM GridEdge	CVE-2022-	gov/vuln/detail/CVE-2022-	/C:N/I: H/A:N	none;HIGH;non	improperly protected file to import	SICAM GridEdge runs, are able to	
Essential GDS ARM	34464	34464	5,5 MEDIUM	е	SSH keys	inject a custom SSH key to that file.	FALSE DATA INJECTION
					Improper Limitation of a Pathname to		
			AV:A/AC:H/PR:N/UI:N/S:		a Restricted Directory ('Path		
ABB zenon 7.50			U/C:H/I: L/A:N		Traversal') - allows the user to	An attacker who successfully exploit	
ABB zenon 7.60			5,9 MEDIUM> ABB		access files on the Zenon system	the vulnerability could access the	
ABB zenon 8.00		https://nvd.nist.	AV:N/AC:L/PR:N/UI:N/S:		and user also can add own log	Zenon runtime activities such as the	
ABB zenon 8.10	CVE-2022-	gov/vuln/detail/CVE-2022-	U/C:H/I: L/A:N	HIGH;LOW;non	messages and e.g., flood the log	start and stop of various activity and	
ABB zenon 8.20	34836	<u>34836</u>	8,2 HIGH> NIST	е	entries.	the last error code etc.	EAVESDROPPING
			AV:L/AC:H/PR:N/UI:N/S:				
ABB zenon 7.50			U/C:H/I: L/A:L			allows an attacker who successfully	
ABB zenon 7.60			6.2 MEDIUM> ABB			exploit the vulnerability may add	
ABB zenon 8.00		https://nvd.nist.	AV:L/AC:L/PR:L/UI:N/S:U		Insufficiently Protected Credentials -	more network clients that may	
ABB zenon 8.10	CVE-2022-	gov/vuln/detail/CVE-2022-	/C:H/I: L/A:N	HIGH;LOW;LO	Storing Passwords in a Recoverable	monitor various activities of the	
ABB zenon 8.20	34837	34837	6,1 MEDIUM> NIST	W	Format	Zenon.	FALSE DATA INJECTION
ADD ZEIIUII O.ZU	34031	<u>34031</u>	O, I WIEDIUWI> NIST	٧V	ruiiiat	Zenon.	FALSE DATA INJECTION

1				_			
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;HIG H	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;non	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;LO W	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;non e	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;LO W	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

		1	1				
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;non e	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;non e	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;non	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;non	Improper Neutralization of Directives in Dynamically Evaluated Code ("Eval Injection")	may allow a remote, unauthenticated	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;non	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.	

		Т	1	ı			
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						may allow a remote unauthorized	
Esri ArcGIS Server 10.6.1 on X64						attacker able to convince a user to	
Esri ArcGIS Server 10.7.1 on X64						click on a crafted link which could	
Esri ArcGIS Server 10.8.1 on X64		https://nvd.nist.	AV:N/AC:L/PR:N/UI:R/S:		Improper Neutralization of Input	potentially execute arbitrary	
Esri ArcGIS Server 10.9.0 on X64	CVE-2022-	gov/vuln/detail/CVE-2022-	C/C:L/I: L/A:N	LOW;LOW;non	During Web Page Generation ('Cross-	JavaScript code in the victim's	
Esri ArcGIS Server 10.9.1 on X64	38195	<u>38195</u>	6,1 MEDIUM	е	site Scripting')	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			AV:N/AC:L/PR:H/UI:N/S:				
Esri ArcGIS Server 10.6.1 on X64			U/C:N/I: H/A:H				
Esri ArcGIS Server 10.7.1 on X64			6,5 MEDIUM> ESRI			may result in a denial of service by	
Esri ArcGIS Server 10.8.1 on X64		https://nvd.nist.	AV:N/AC:L/PR:L/UI:N/S:		Improper Limitation of a Pathname to	allowing a remote, authenticated	
Esri ArcGIS Server 10.9.0 on X64	CVE-2022-	gov/vuln/detail/CVE-2022-	U/C:N/I: H/A:H	none;HIGH;HIG	a Restricted Directory ('Path	attacker to overwrite internal ArcGIS	
Esri ArcGIS Server 10.9.1 on X64	38196	<u>38196</u>	8,1 HIGH> NIST	Н	Traversal')	Server directory	DENIAL OF SERVICE

		l	I				
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						may allow a remote, unauthenticated	
on X64						attacker to phish a user into	
Esri ArcGIS Server 10.6.1 on X64						accessing an attacker controlled	
Esri ArcGIS Server 10.7.1 on X64						website via a crafted query	
Esri ArcGIS Server 10.8.1 on X64		https://nvd.nist.	AV:N/AC:L/PR:N/UI:R/S:			parameter. It could lead to credential	
Esri ArcGIS Server 10.9.0 on X64	CVE-2022-	gov/vuln/detail/CVE-2022-	C/C:L/I: L/A:N	LOW;LOW;non	URL Redirection to Untrusted Site	theft, malware distribution or other	
Esri ArcGIS Server 10.9.1 on X64	38197	38197	6,1 MEDIUM	е	('Open Redirect')	advanced attack	OTHER
Esri ArcGIS Server on X64						may allow a remote,	
Esri ArcGIS Server 10.6.1 on X64						unauthenticated attacker to	
Esri ArcGIS Server 10.0.1 on X64						convince a user to click on a crafted	
Esri ArcGIS Server 10.7.1 on X64		https://nvd.nist.	AV:N/AC:L/PR:N/UI:R/S:		Improper Neutralization of Input	link which could potentially execute	
Esri ArcGIS Server 10.9.0 on X64	CVE-2022-	gov/vuln/detail/CVE-2022-	C/C:L/I: L/A:N	LOW;LOW;non		' '	
Esri ArcGIS Server 10.9.1 on X64	38198	38198	6,1 MEDIUM	LOVV,LOVV,IIOII	site Scripting')	victim's browser	OTHER
ESTI AICOIS Server 10.9.1 OII X04	30190	30190	O, I WEDIOW	6	site Scripting)	Victim's blowsei	OTTLER
						may in some edge cases allow a	
						remote, unauthenticated attacker to	
Esri ArcGIS Server 10.7.1 on X64		https://nvd.nist.	AV:N/AC:L/PR:N/UI:R/S:			induce an unsuspecting victim to	
Esri ArcGIS Server 10.8.1 on X64	CVE-2022-	gov/vuln/detail/CVE-2022-	C/C:L/I: L/A:N	LOW;LOW;non	Download of Code Without Integrity	launch a process in the victim's	
Esri ArcGIS Server 10.9.1 on X64	38199	38199	6,1 MEDIUM	е	Check	PATH environment.	OTHER
Esri ArcGIS Server 10.7.1 Esri							
ArcGIS Server 10.8.1		https://nvd.nist.	AV:N/AC:L/PR:N/UI:R/S:		Improper Neutralization of Input	Specifically crafted web requests	
Esri ArcGIS Server 10.7.1 on X64	CVE-2022-	gov/vuln/detail/CVE-2022-	C/C:L/I: L/A:N	LOW;LOW;non	During Web Page Generation ('Cross-	can execute arbitrary JavaScript in	
Esri ArcGIS Server 10.8.1 on X64	38200	38200	6,1 MEDIUM	е	site Scripting')	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						may allow a remote, unauthenticated	
on X64						attacker traverse the file system to	
Esri ArcGIS Server 10.6.1 on X64						access files outside of the intended	
Esri ArcGIS Server 10.7.1 on X64						directory on ArcGIS Server. This	
Esri ArcGIS Server 10.8.1 on X64		https://nvd.nist.	AV:N/AC:L/PR:N/UI:N/S:		Improper Limitation of a Pathname to	could lead to the disclosure of	
Esri ArcGIS Server 10.9.0 on X64	CVE-2022-	gov/vuln/detail/CVE-2022-	U/C:H/I: N/A:N	HIGH;none;non	a Restricted Directory ('Path	sensitive site configuration	
Esri ArcGIS Server 10.9.1 on X64	38202	38202	7,5 HIGH	е	Traversal')	information (not user datasets).	EAVESDROPPING
Esri Portal For Arcgis							
Esri Portal For Arcgis 10.6 Esri							
Portal For Arcgis 10.6.1 Esri Portal						may allow a remote, unauthenticated	
For Arcgis 10.7.1 Esri Portal For						attacker to forge requests to arbitrary	
Arcgis 10.8 Esri Portal For Arcgis						URLs from the system, potentially	
10.8.1		https://nvd.nist.	AV:N/AC:L/PR:N/UI:N/S:		Protections against potential Server-	leading to network enumeration or	
	CVE-2022-	gov/vuln/detail/CVE-2022-	U/C:H/I: N/A:N		Side Request Forgery (SSRF) were	reading from hosts inside the	
x64	38203	<u>38203</u>	7,5 HIGH	е	not fully honored	network perimeter,	EAVESDROPPING
						may allow a remote, unauthenticated	
						attacker to create a crafted link	
Esri Portal For Arcgis 10.7.1 Esri		https://nvd.nist.	AV:N/AC:L/PR:N/UI:R/S:		Improper Neutralization of Input	which when clicked could potentially	
Portal For Arcgis 10.8.1 Esri Portal	CVE-2022-	gov/vuln/detail/CVE-2022-	C/C:L/I: L/A:N	LOW;LOW;non	During Web Page Generation ('Cross-	execute arbitrary JavaScript code in	
For Arcgis 10.8.1 on x64	38204	38204	6,1 MEDIUM	е	site Scripting') - reflected XSS	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						may allow a remote, unauthenticated	
Esri Portal For Arcgis 10.9 Esri						attacker to traverse the file system	
Portal For Arcgis 10.9.1		https://nvd.nist.	AV:N/AC:L/PR:N/UI:N/S:			and lead to the disclosure of	
Esri Portal For Arcgis 10.9.1 on	CVE-2022-	gov/vuln/detail/CVE-2022-	U/C:H/I: N/A:N	HIGH;none;non		sensitive data (not customer-	
x64	38205	38205	7,5 HIGH	е	directory traversal issue	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						may allow a remote remote,	
Portal For Arcgis 10.9.1						unauthenticated attacker to create a	
Esri Portal For Arcgis 10.9.1 on		https://nvd.nist.	AV:N/AC:L/PR:N/UI:R/S:			crafted link which when clicked	
x64	CVE-2022-	gov/vuln/detail/CVE-2022-	C/C:L/I: L/A:N	LOW;LOW;non		could execute arbitrary JavaScript	
Esri Portal For Arcgis 11.0	38206	38206	6,1 MEDIUM	е	reflected XSS vulnerability	code in the victim's browser.	OTHER
						may allow a remote remote,	
						unauthenticated attacker to create a	
						crafted link which when clicked	
Esri Portal For Arcgis 10.7.1 Esri		https://nvd.nist.	AV:N/AC:L/PR:N/UI:R/S:		Improper Neutralization of Input	which could execute arbitrary	
Portal For Arcgis 10.8.1 Esri Portal	CVE-2022-	gov/vuln/detail/CVE-2022-	C/C:L/I: L/A:N	LOW;LOW;non	During Web Page Generation ('Cross-	JavaScript code in the victim's	
For Arcgis 10.8.1 on x64	38207	<u>38207</u>	6,1 MEDIUM	е	site Scripting') - reflected XSS	browser.	OTHER

<u> </u>	1	ī	T				
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						may allow a remote, unauthenticated	
Portal For Arcgis 10.9.1						attacker to craft a URL that could	
Esri Portal For Arcgis 10.9.1 on		https://nvd.nist.	AV:N/AC:L/PR:N/UI:R/S:			redirect a victim to an arbitrary	
x64	CVE-2022-	gov/vuln/detail/CVE-2022-	C/C:L/I: L/A:N	LOW:LOW:non	URL Redirection to Untrusted Site	website, simplifying phishing	
Esri Portal For Arcgis 11.0	38208	38208	6,1 MEDIUM	е	('Open Redirect')	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						which may allow a remote,	
Esri Portal For Arcgis 10.9 Esri						unauthenticated attacker to create a	
Portal For Arcgis 10.9.1		https://nvd.nist.	AV:N/AC:L/PR:N/UI:R/S:		Improper Neutralization of Input	crafted link which when clicked	
Esri Portal For Arcgis 10.9.1 on	CVE-2022-	gov/vuln/detail/CVE-2022-	C/C:L/I: L/A:N	LOW;LOW;non	During Web Page Generation ('Cross-	could execute arbitrary JavaScript	
x64	38209	<u>38209</u>	6,1 MEDIUM	е	site Scripting') - reflected XSS	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						may allow a remote, unauthenticated	
Esri Portal For Arcgis 10.9 Esri						attacker to create a crafted link	
Portal For Arcgis 10.9.1		https://nvd.nist.	AV:N/AC:L/PR:N/UI:R/S:			which when clicked could render	
Esri Portal For Arcgis 10.9.1 on	CVE-2022-	gov/vuln/detail/CVE-2022-	C/C:L/I: L/A:N	LOW;LOW;non	reflected HTML injection	arbitrary HTML in the victim's	
x64	38210	38210	6,1 MEDIUM	е	vulnerability	•	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						many all any a remarks type of booking to d	
=					Dtti	may allow a remote, unauthenticated	
x64					Protections against potential Server-	attacker to forge requests to arbitrary	
Esri Portal For Arcgis 10.9 Esri					Side Request Forgery (SSRF)	URLs from the system, potentially	
Portal For Arcgis 10.9.1	0.45 0000	https://nvd.nist.	AV:N/AC:L/PR:N/UI:N/S:		vulnerabilities in Esri Portal for	leading to network enumeration or	
Esri Portal For Arcgis 10.9.1 on	CVE-2022-	gov/vuln/detail/CVE-2022-	U/C:H/I: N/A:N	HIGH;none;non	ArcGIS versions 10.9.1 and below	reading from hosts inside the	
x64	38211	<u>38211</u>	7,5 HIGH	е	were not fully honored	network perimeter	EAVESDROPPING
Esri Portal For Arcgis							
Esri Portal For Arcgis 10.6 Esri							
Portal For Arcgis 10.6.1 Esri Portal						may allow a remote, unauthenticated	
· ·					Dratactions against natential Conver		
For Arcgis 10.7.1 Esri Portal For					Protections against potential Server-	attacker to forge requests to arbitrary	
Arcgis 10.8 Esri Portal For Arcgis		https://nvd.nist.	AV:N/AC:L/PR:N/UI:N/S:		Side Request Forgery (SSRF)	URLs from the system, potentially	
10.8.1	0) (5,000				vulnerabilities in Esri Portal for	leading to network enumeration or	
Esri Portal For Arcgis 10.8.1 on	CVE-2022-	gov/vuln/detail/CVE-2022-	U/C:H/I: N/A:N	HIGH;none;non	ArcGIS versions 10.8.1 and below	reading from hosts inside the	aa
x64	38212	38212	7,5 HIGH	е	were not fully honored	network perimeter,	EAVESDROPPING
Siemens SIMATIC S7-1200 CPU							
12 1211C							
Siemens SIMATIC S7-1200 CPU							
12 1212C							
Siemens SIMATIC S7-1200 CPU							
12 1212fc						could allow attackers to discover	
Siemens SIMATIC S7-1200 CPU						the private key of a CPU product	
12 1214C						family by an offline attack against a	
Siemens SIMATIC S7-1200 CPU			AV:L/AC:L/PR:N/UI:N/S:			single CPU of the family.	
12 1214fc			C/C:H/I: H/A:H			Attackers could then use this	
Siemens SIMATIC S7-1200 CPU			9,3 CRITICAL>			knowledge to extract confidential	
12 1215C			SIEMENS			configuration data from projects that	
Siemens SIMATIC S7-1200 CPU		https://nvd.nist.	AV:L/AC:L/PR:L/UI:N/S:U			are protected by that key or to	
12 1215fc	CVE-2022-	gov/vuln/detail/CVE-2022-	/C:H/I: H/A:H	HIGH;HIGH;HIG		perform attacks against legacy	
Siemens SIMATIC S7-1200 CPU	38465	38465	7,8 HIGH> NIST	Н	Insufficiently Protected Credentials	PG/PC and HMI communication.	EAVESDROPPING
			AV:N/AC:H/PR:N/UI:R/S:				
			U/C:H/I: H/A:H				
	I		7,5 HIGH> SIEMENS		Session Fixation - Affected devices		
						I	
		https://nvd.nist.	AV:N/AC:L/PR:L/UI:N/S:		accept user defined session cookies	This could allow an attacker to take	
SICAM P850 	CVE-2022- 40226	https://nvd.nist. gov/vuln/detail/CVE-2022- 40226	AV:N/AC:L/PR:L/UI:N/S: U/C:H/I: H/A:N 8.1 HIGH> NIST	HIGH;HIGH;HIG	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;HIG H	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		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;HIG H	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		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;HIG H	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;HIG H	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

		ı	1	ı			
						transmits the database credentials for the inbuilt SQL server in cleartext.	
						In combination with the by default	
Siemens SICAM PAS (Power						enabled xp cmdshell feature	
Automation System)		https://nvd.nist.	AV:N/AC:L/PR:N/UI:N/S:			unauthenticated remote attackers	
Automation System)	CVE-2022-	gov/vuln/detail/CVE-2022-	U/C:H/I: H/A:H	nich-nich-nic	Cleartext Transmission of Sensitive	could execute custom OS	
Siemens SICAM PQS	43724	43724	9,8 CRITICAL	i iiGi i,i iiGi i,i iiG	Information	commands	COMMAND INJECTION
Siemens Sicalii FQS	43724	43724	9,0 CRITICAL		Information	Commanus	COMMAND INSECTION
			AV:N/AC:L/PR:N/UI:N/S:				
			U/C:N/I: N/A:H				
			7,5 HIGH > NIST		Uncontrolled Resource Consumption		
			AV:N/AC:L/PR:N/UI:N/S:		- Affected devices do not properly	This could allow an attacker to	
		https://nvd.nist.	U/C:N/I: N/A:L		restrict secure client-initiated	create a denial of service condition	
	CVE-2022-	gov/vuln/detail/CVE-2022-	5,3 MEDIUM>	none;none;HIG	renegotiations within the SSL and	on the ports 443/tcp and 4443/tcp for	
SIPROTEC	45044	<u>45044</u>	SIEMENS	Н	TLS protocols.	the duration of the attack.	DENIAL OF SERVICE
						may allow a remote, unauthenticated	
						attacker to craft a URL that could	
Esri Portal For Arcgis 10.9.1 Esri		https://nvd.nist.	AV:N/AC:L/PR:N/UI:R/S:			redirect a victim to an arbitrary	
Portal For Arcgis 10.9.1 on x64	CVE-2023-	gov/vuln/detail/CVE-2023-	C/C:L/I: L/A:N	LOW;LOW;non	URL Redirection to Untrusted Site	website, simplifying phishing	
Esri Portal For Arcgis 11.0	25829	25829	6,1 MEDIUM	e	('Open Redirect')	attacks.	OTHER
			-,				-
Esri Portal For Arcgis 10.7.1 Esri						may allow a remote, unauthenticated	
Portal For Arcgis 10.8.1 Esri Portal		hatter a collection of the first	ANAMA OLI /DD-M/UU-D/O		lasana an Nasataalia ati an af lasant	attacker to create a crafted link	
For Arcgis 10.8.1 on x64	C)/E 2022	https://nvd.nist.	AV:N/AC:L/PR:N/UI:R/S:	L OWAL OWARS	Improper Neutralization of Input	which when clicked could potentially	
Esri Portal For Arcgis 10.9.1 Esri	CVE-2023-	gov/vuln/detail/CVE-2023-	C/C:L/I: L/A:N	LOW;LOW;non	During Web Page Generation ('Cross-	· '	OTHER
Portal For Arcgis 10.9.1 on x64	25830	<u>25830</u>	6,1 MEDIUM	е	site Scripting') - reflected XSS	the victim's browser.	OTHER
Esri Portal For Arcgis 10.7.1 Esri						may allow a remote, unauthenticated	
Portal For Arcgis 10.8.1 Esri Portal						attacker to create a crafted link	
For Arcgis 10.8.1 on x64		https://nvd.nist.	AV:N/AC:L/PR:N/UI:R/S:		Improper Neutralization of Input	which when clicked could potentially	
Esri Portal For Arcgis 10.9.1 Esri	CVE-2023-	gov/vuln/detail/CVE-2023-	C/C:L/I: L/A:N	LOW;LOW;non	During Web Page Generation ('Cross-	execute arbitrary JavaScript code in	
Portal For Arcgis 10.9.1 on x64	25831	<u>25831</u>	6,1 MEDIUM	е	site Scripting') - reflected XSS	the victim's browser.	OTHER

Ford Double For America							
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 Esti							
Esri Portal For Arcgis 10.9.1 on		https://nvd.nist.	AV:N/AC:L/PR:N/UI:R/S:			may allow an attacker to trick an	
x64	CVE-2023-	gov/vuln/detail/CVE-2023-		nich-nich-nic	cross-site-request forgery	authorized user into executing	
Esri Portal For Arcgis 11.0	25832	25832	8,8 HIGH	HIGH;HIGH;HIG	vulnerability	unwanted actions	COMMAND INJECTION
LSII FOILAI FOI AICGIS TT.0	23032	23632	0,0 111011	11	vullerability	unwanted actions	COMMAND INSECTION
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						may allow a remote, authenticated	
Esri Portal For Arcgis 10.9 Esri						attacker to create a crafted link	
Portal For Arcgis 10.9.1		,,	AVAN/A O L /DD L /III D/O			which when clicked could render	
Esri Portal For Arcgis 10.9.1 on	0)/5 0000	https://nvd.nist.	AV:N/AC:L/PR:L/UI:R/S:			arbitrary HTML in the victim's	
x64	CVE-2023-	gov/vuln/detail/CVE-2023-	C/C:L/I: L/A:N	LOW;LOW;non		browser (no stateful change made or	OTUED
Esri Portal For Arcgis 11.0	25833	<u>25833</u>	5,4 MEDIUM	е	HTML injection vulnerability	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		https://nvd.nist.	AV:N/AC:L/PR:L/UI:N/S:			may allow users to access content	
Esri Portal For Arcgis 10.9.1 on	CVE-2023-	gov/vuln/detail/CVE-2023-	U/C:L/I: L/A:N	LOW;LOW;non		that they are no longer privileged to	LATERAL MOVEMENT

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						The attack could disclose a	
Esri Portal For Arcgis 10.9.1 on		https://nvd.nist.	AV:N/AC:L/PR:H/UI:R/S:		Improper Neutralization of Input	privileged token which may result	
x64	CVE-2023-	gov/vuln/detail/CVE-2023-	C/C:L/I: L/A:N	LOW;LOW;non	During Web Page Generation ('Cross-	the attacker gaining full control of the	
Esri Portal For Arcgis 11.0	25835	<u>25835</u>	4,8 MEDIUM	е	site Scripting')	Portal.	ACCESS
Esri Portal For Arcgis 10.7.1 Esri						may allow a remote, authenticated	
Portal For Arcgis 10.8.1 Esri Portal						attacker to create a crafted link	
For Arcgis 10.8.1 on x64		https://nvd.nist.	AV:N/AC:L/PR:L/UI:R/S:		Improper Neutralization of Input	which when clicked could potentially	
Esri Portal For Arcgis 10.9.1 Esri	CVE-2023-	gov/vuln/detail/CVE-2023-	C/C:L/I: L/A:N		During Web Page Generation ('Cross-	· · · · · · · · · · · · · · · · · · ·	
Portal For Arcgis 10.9.1 on x64	25836	25836	5,4 MEDIUM		site Scripting')	the victims browser	OTHER
<u> </u>					. 57		
						may allow a remote, authenticated	
						attacker to create a crafted link	
Esri Portal For Arcgis 10.8.1 Esri		https://nvd.nist.	AV:N/AC:L/PR:H/UI:R/S:		Improper Neutralization of Input	which when clicked could potentially	
Portal For Arcgis 10.8.1 on x64	CVE-2023-	gov/vuln/detail/CVE-2023-	C/C:L/I: L/A:N	LOW;LOW;non	During Web Page Generation ('Cross-	execute arbitrary JavaScript code in	
Esri Portal For Arcgis 10.9	25837	<u>25837</u>	4,8 MEDIUM	е	site Scripting')	the victims browser.	OTHER
						may allow a remote, authenticated	
						attacker to create a crafted link	
		https://nvd.nist.	AV:N/AC:L/PR:H/UI:R/S:		Improper Neutralization of Input	which onmouseover wont execute	
	CVE-2023-	gov/vuln/detail/CVE-2023-	C/C:N/I: L/A:N	none;LOW;non	During Web Page Generation ('Cross-	but could potentially render an	
ESRI ArcGIS 10.8.1	25840	25840	3,4 LOW	е	site Scripting')	image in the victims browser	OTHER
						_	
						may allow a remote, unauthenticated	
						attacker to create crafted content	
		https://nvd.nist.	AV:N/AC:L/PR:N/UI:R/S:		Improper Neutralization of Input	which when clicked could potentially	
	CVE-2023-	gov/vuln/detail/CVE-2023-	C/C:L/I: L/A:N	LOW;LOW;non	During Web Page Generation ('Cross-	· '	
ESRI ArcGIS 10.8.1	25841	<u>25841</u>	6,1 MEDIUM	е	site Scripting')	the victim's browser.	OTHER
					NULL Pointer Dereference - Affected	An unauthenticated remote attacker	
		https://nvd.nist.	AV:N/AC:L/PR:N/UI:N/S:		devices lack proper validation of http	could send specially crafted packets	
	CVE-2023-	gov/vuln/detail/CVE-2023-	U/C:N/I: N/A:H		request parameters of the hosted	that could cause denial of service	

			1				
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;LO	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
Control Lack - Opunio C	20020		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		oomen.e.	vaniolazinty man row ondoanty	7.00200
					Incorrect Permission Assignment for Critical Resource - Affected applications fail to set proper access		
		https://nvd.nist.	AV:L/AC:L/PR:L/UI:N/S:U		rights for their installation folder if a	This could allow an authenticated	COMMAND INJECTION
	CVE-2023-	gov/vuln/detail/CVE-2023-	/C:H/I: H/A:H	HIGH;HIGH;HIG	non-default installation path was	local attacker to inject arbitrary code	LATERAL MOVEMENT /
Siemens WinCC 7.4	30897	30897	7,8 HIGH	H	chosen during installation	and escalate privileges.	PRIVILEGE ESCALATION
			AV:N/AC:L/PR:N/UI:R/S: U/C:N/I: L/A:N 4,3 MEDIUM>			By tricking an authenticated victim	
			SIEMENS		Cross-Site Request Forgery (CSRF) -	user to click a malicious link, an	
	0) (5,000	https://nvd.nist.	AV:N/AC:L/PR:N/UI:R/S:	1.004	The web interface of the affected	attacker could perform arbitrary	
SICAM Q200	CVE-2023- 30901	gov/vuln/detail/CVE-2023-	U/C:H/I: H/A:H 8.8 HIGH> NIST	none;LOvv;non		actions on the device on behalf of	COMMAND IN IT CTION
SICAIVI UZUU	30901	30901	O,O TIGH> INIO I	е	Request Forgery attacks.	the victim user.	COMMAND INJECTION
			AV:N/AC:H/PR:L/UI:R/S:				
			C/C:L/I: L/A:L				
			5,5 MEDIUM>				
			SIEMENS		Incorrect Permission Assignment for	· ·	
		https://nvd.nist.	AV:N/AC:H/PR:N/UI:N/S:		Critical Resource - Affected devices	session token can use it to	
	CVE-2023-	gov/vuln/detail/CVE-2023-	U/C:L/I: L/A:N	LOW;LOW;LO	are missing cookie protection flags	impersonate a legitimate application	
SICAM Q200	31238	<u>31238</u>	4,8 MEDIUM> NIST	W	when using the default settings	user	ACCESS

						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	
			AV:L/AC:H/PR:L/UI:N/S:			and need to access the system via	
ABB zenon 7.50			U/C:H/I: H/A:H		External Control of System or	various means some of the zenon	
ABB zenon 7.60			7,0 HIGH> ABB		Configuration Setting - allowing low-	directories are accessible for low	
ABB zenon 8.00			AV:N/AC:L/PR:L/UI:N/S:		privileged users to read and update	privileged users. These directories	
ABB zenon 8.10	CVE-2023-	https://nvd.nist.	U/C:H/I: H/A:H	HIGH;HIGH;HIG	the data in various directories used	may be used further to carry out the	FALSE DATA INJECTION
ABB zenon 8.20	3321	gov/vuln/detail/CVE-2023-3321	8,8 HIGH> NIST	Н	by the Zenon system	attacks.	EAVESDROPPING
						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	
			AV:L/AC:H/PR:L/UI:N/S:			and need to access the system via	
ABB zenon 7.50			U/C:H/I: H/A:H		Incorrect Permission Assignment for	various means some of the zenon	
ABB zenon 7.60			7,0 HIGH> ABB		Critical Resource - allowing low-	directories are accessible for low	
ABB zenon 8.00			AV:N/AC:L/PR:L/UI:N/S:		privileged users to read and update	privileged users. These directories	
ABB zenon 8.10	CVE-2023-	https://nvd.nist.	U/C:H/I: H/A:N	HIGH;HIGH;HIG	the data in various directories used	may be used further to carry out the	FALSE DATA INJECTION
ABB zenon 8.20	3322	gov/vuln/detail/CVE-2023-3322	8,1 HIGH> NIST	Н	by the Zenon system	attacks.	EAVESDROPPING

						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	
			AV:P/AC:H/PR:L/UI:N/S:			and need to access the system via	
ABB zenon 7.50			U/C:L/I: H/A:H		Incorrect Default Permissions -	various means some of the zenon	
ABB zenon 7.60			5,9 MEDIUM> ABB		allowing low-privileged users to read	directories are accessible for low	
ABB zenon 8.00			AV:N/AC:L/PR:L/UI:N/S:		and update the data in various	privileged users. These directories	
ABB zenon 8.10	CVE-2023-	https://nvd.nist.	U/C:L/I: L/A:N	LOW;HIGH;HIG	directories used by the Zenon	may be used further to carry out the	FALSE DATA INJECTION
ABB zenon 8.20	3323	gov/vuln/detail/CVE-2023-3323	5,4 MEDIUM> NIST	Н	system	attacks.	EAVESDROPPING
						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	
			AV:L/AC:H/PR:L/UI:R/S:			and need to access the system via	
ABB zenon 7.50			U/C:L/I: H/A:H		Deserialization of Untrusted Data	various means some of the zenon	
ABB zenon 7.60			6,3 MEDIUM> ABB		- allowing low-privileged users to	directories are accessible for low	
ABB zenon 8.00			AV:N/AC:H/PR:L/UI:N/S:		read and update the data in various	privileged users. These directories	
ABB zenon 8.10	CVE-2023-	https://nvd.nist.	U/C:H/I: H/A:H	LOW;HIGH;HIG	directories used by the Zenon	may be used further to carry out the	FALSE DATA INJECTION
ABB zenon 8.20	3324	gov/vuln/detail/CVE-2023-3324	7,5 HIGH > NIST	Н	system	attacks.	EAVESDROPPING