ICS/SCADA/PLC Google/Shodanhq Cheat Sheet

Gleb Gritsai, Alexander Timorin, Yuri Goltsev, Roman Ilin

http://scadastrangelove.org/

vendor	product	google dork	network info
Siemens	S7-200		all models: tcp/udp/102 (by vuln info)
	S7-300		snmp: Siemens, SIMATIC, S7
	S7-3** , PCS7	inurl:/Portal0000.htm	http: /S7Web.css
	Simatic S7		snmp: Siemens, SIMATIC S7, CPU-1200 Siemens, **SIMATIC** S7, CPU317-2 PN/DP Siemens, **SIMATIC** S7, CPU315-2 PN/DP

	Siemens, **SIMATIC** S7 ***
inurl:"Portal/Portal.mwsl"	http: /S7Web.css
Automation License Manager	tcp/4410 (by vuln info)
Scalance S,X Security Module firewall	telnet: Simatic, Scalance snmp: Scalance S*, Scalance W*, Scalance X* DCP protocol (by vuln info) tcp/80
Wincc flexible Wincc flexible runtime / TIA Portal	netbios: WINCC_SRV21 <0x0> SIEMENS <0x0> WINCC_SRV21 <0x20> tcp/2308 (by vuln info) tcp/50523 (by vuln info)

Synco OZW (Web server)		http
SIMATIC HMI Miniweb	intitle:"Miniweb Start Page" | "/CSS/Miniweb.css"	http: /CSS/Miniweb.css
Simatic HMI		snmp: Siemens, SIMATIC HMI, ***
		telnet:Welcome to the Windows CE Telnet Service on HMI_Panel

vendor	product	google dork	network info
Emerson	DeltaV and DeltaV Workstations/DeltaV ProEssentials Scientific Graph		tcp/udp/111 (by vuln info)
	DeltaV Service Information System Ver3.3		

vendor	product	google dork	network info
Allen-Bradley Rockwell Automation			
	ControlLogix		tcp/udp/44818 , http
	CompactLogix	intitle:"Rockwell Automation" "Device Name" "Uptime"	

PLC5		http, snmp
SLC-5	inurl:dtm.html intitle:1747-L552 inurl:dtm.html intitle:1747-L551	http, snmp
Micrologix	inurl:home.htm intitle:1766	http, snmp

vendor	product	shodanhq dork	network info
Schneider Electric			
	PM820SD	Schneider Electric - PM820SD port:161	
	PM870SD	Schneider Electric - PM870SD port:161	
	ECC21	Schneider Electric - ECC21 port:161	
	EGX100MG	Schneider Electric - EGX100MG port:161	
	PowerLogic PM800	PowerLogic PM800 port:80	
	PowerLogic ION8650 A/B/C	ION8650	

PowerLogic ION8650 A/B/C)	8650 ION
PowerLogic ION8600	8600 ION
PowerLogic ION7650/7550	ION 7550
PowerLogic ION7650/7550	ION 7650
PowerLogic ION7300	ION 7300
PowerLogic ION6200	ION6200
PowerLogic PM1200	PM1200
PowerLogic DM6200	DM6200
Powerlogic Enercept	
Powerlogic Energy Meter	
PowerLogic Branch Current Monitor	BCM42
PowerLogic EM4800	

PowerLogic E5600	
PowerLogic Ethernet Gateway (EGX)	EGX100
PowerLogic EGX300	EGX300
PowerLogic ION7550RTU	ION 7550RTU schneider electric

vendor	product	google dork	network info
Schneider Electric			
	Modicon Quantum/Premiun/Micro	intitle:"Quantum CPU Web Server" intitle:"Premium CPU Web Server"	
	CitectSCADA CitectFacilities	intitle:"Citect Web" inurl:scada filetype:htm	
	ClearSCADA	shodanhq: ClearSCADA "ViewXCtrl is not supported in this web browser." intitle:"ClearSCADA Home"	
	UnitelWay Device Driver		

	Vijeo Historian Web Server	several products	
	Modicon M340		snmp: "Modicon M340"

vendor	product	google dork	network info
General Electric			
	Cimplicity	intitle:"CIMPLICITY WebView" inurl:main.html	http
	Proficy	inurl:ProficyPortal/default.asp	http