Montage_Anlagennetz

192.168.30.0/24 | Staged scan complete | Scan 10.11.2026 14:20, duration 1 h 28 min.

Traffic light YELLOW: Action required

Some devices offer services that are considered insecure. This is not an attack, but an open door that should be closed in a planned way.

22	19	38	2
Devices found	with insecure service	insecure services	only in firewall traffic

Key points

- 22 devices were found in network Montage_Anlagennetz.
- 19 of 22 devices offer at least one insecure service.
- 9 devices are affected according to vendor advisories (firmware in the affected range); for 2 devices, the model matches an advisory - check the firmware on the device.
- 2 devices are visible only in firewall traffic (Splunk 02.11.2026 - 08.11.2026), not in the scan - 2 of them not in the CMDB.
- 38 of 38 insecure services had no traffic through the firewall during the Splunk period 02.11.2026 - 08.11.2026 - candidates for disabling.
- Most common: HTTP on 15 devices, SNMP on 10 devices, Telnet on 5 devices.
- Most devices are: Controller (PLC) (13 of 22).

What needs to be done?

1. HTTP on 15 devices: Switch to HTTPS or disable; logging in over HTTP is not permitted under the traffic rules.
2. SNMP on 10 devices: SNMPv1/v2c and 'public' are not permitted under the traffic rules: switch to SNMPv3.
3. Telnet on 5 devices: Not permitted under the traffic rules: disable, use SSH for remote access.
4. FTP on 2 devices: Not permitted under the traffic rules: disable, otherwise use SFTP or FTPS.
5. Check firewall rules: allow insecure services only for the computers that really need them.
6. Search the network for 2 Splunk-only devices (MAC/switchport) and add them to the CMDB - template: file "..._CMDB-Nachtrag.xlsx".

Change since the last full scan

No complete previous scan of this network available for comparison.

Insecure services

Assessed according to the traffic rules (HanselCraft default, customizable). An insecure service is not an attack, but an open door that should be closed in a planned way.

Service	Devices	Why risky	What to do
HTTP (TCP 80)	15	Login and settings are sent unencrypted over the network.	Switch to HTTPS or disable; logging in over HTTP is not permitted under the traffic rules.
SNMP (UDP 161)	10	With v1/v2c, the password (community) is sent unencrypted over the network.	SNMPv1/v2c and 'public' are not permitted under the traffic rules: switch to SNMPv3.
Telnet (TCP 23)	5	Passwords and commands are sent unencrypted over the network.	Not permitted under the traffic rules: disable, use SSH for remote access.
FTP (TCP 21)	2	User name, password and files are sent unencrypted over the network.	Not permitted under the traffic rules: disable, otherwise use SFTP or FTPS.

Service	Devices	Why risky	What to do
SMB (TCP 445)	2	Old versions (SMBv1) are a common path for malware.	Disable SMBv1 (not permitted under the traffic rules), use SMBv3 with signing, restrict access.
VNC (TCP 5900)	2	Screen, input and often the password are sent unencrypted over the network.	Not permitted under the traffic rules: disable or use only encrypted (TLS, VPN, SSH tunnel).
RPC (TCP 135)	2	Common attack point; shows which Windows services are running.	Only if technically necessary and only for approved computers; otherwise block via firewall.

Open but not used through the firewall (Splunk 02.11.2026 - 08.11.2026): 38 insecure services without permitted traffic. These are the first candidates for disabling. Splunk only sees traffic through the firewall, not within the network - clarify with the plant owner beforehand.

Service	open	no traffic	Addresses without traffic
HTTP (TCP 80)	15	15	192.168.30.3, 192.168.30.4, 192.168.30.10, 192.168.30.11, 192.168.30.15, 192.168.30.16, 192.168.30.20, 192.168.30.21, 192.168.30.22, 192.168.30.25, 192.168.30.26, 192.168.30.30, 192.168.30.31, 192.168.30.101, 192.168.30.102
SNMP (UDP 161)	10	10	192.168.30.1, 192.168.30.2, 192.168.30.3, 192.168.30.4, 192.168.30.10, 192.168.30.11, 192.168.30.20, 192.168.30.30, 192.168.30.31, 192.168.30.102
Telnet (TCP 23)	5	5	192.168.30.3, 192.168.30.4, 192.168.30.30, 192.168.30.31, 192.168.30.102
FTP (TCP 21)	2	2	192.168.30.20, 192.168.30.22
RPC (TCP 135)	2	2	192.168.30.60, 192.168.30.61
SMB (TCP 445)	2	2	192.168.30.60, 192.168.30.61
VNC (TCP 5900)	2	2	192.168.30.25, 192.168.30.26

Known vulnerabilities (vendor advisories)

Comparison of the detected models and firmware versions with the vendors' security advisories (Siemens, Bosch, CERT@VDE, CISA, etc., as of 2026-10-27). "exact" = firmware is in the affected range, "model" = model matches, firmware unknown or not comparable - check on the device. KEV = actively exploited according to CISA.

Advisory	Model / firmware	Devices	CVSS	KEV	Quality	Vendor-recommended action
SSA-452276	CPU 1516-3 PN/DP 2.9.4	1	9.6	-	exact	Update to V2.9.9 or later version
SSA-591731	CPU 1516-3 PN/DP 2.9.4	1	9.6	-	exact	Disable the webserver if not required on the affected systems. Restrict the access to Port 80/tcp and 443/tcp to trusted IP address only
SSA-688146	CPU 1516-3 PN/DP 2.9.4	1	9.1	-	exact	Restrict TIA project download to trusted personnel only.
SSA-699386	SCALANCE XC208 6GK5 208-0BA00-2AC2 V4.3	1	9.1	-	exact	Update to V4.5 or later version
SSA-710008	SCALANCE XC208 6GK5 208-0BA00-2AC2 V4.3	1	9.1	-	exact	Update to V4.4 or later version
SSA-723487	SCALANCE XC208 6GK5 208-0BA00-2AC2 V4.3	1	9.0	-	exact	Update to V4.6 or later version
SSA-552702	SCALANCE XC208 6GK5 208-0BA00-2AC2 V4.3	1	8.8	-	exact	Update to V4.4 or later version
SSA-224824	CPU 1214C DC/DC/DC 4.2.3; CPU 1214C DC/DC/DC 4.4.1; CPU 1215	3	7.5	-	exact	Update to V4.7 or later version
SSA-349422	CPU 315-2 PN/DP 3.2.14; CPU 317-2 PN/DP 3.2.15	2	7.5	-	exact	Update to V3.2.17 or later version
SSA-382653	CPU 1516-3 PN/DP 2.9.4	1	7.5	-	exact	Update to V2.9.7 or later version
SSA-392349	CPU 1516-3 PN/DP 2.9.4; CPU 315-2 PN/DP 3.2.14; CPU 317-2 PN	3	7.5	-	exact	As a mitigation, disable the ethernet ports on the CPU and use a communication module (like CP) for communication instead
SSA-473245	CMDB: Siemens TP1200 Comfort V16; CPU 315-2 PN/DP 3.2.14; CP	4	7.5	-	exact	Restrict network access to affected devices
SSA-480230	CPU 315-2 PN/DP 3.2.14; CPU 317-2 PN/DP 3.2.15; SIMATIC HMI	3	7.5	-	exact	Update to V3.2.16 or later version

Advisory	Model / firmware	Devices	CVSS	KEV	Quality	Vendor-recommended action
SSA-592380	CPU 1516-3 PN/DP 2.9.4	1	7.5	-	exact	Limit access to port 102/tcp to trusted users and systems only
SSA-593272	CPU 315-2 PN/DP 3.2.14; CPU 317-2 PN/DP 3.2.15	2	7.5	-	exact	Currently no fix is planned

35 more advisories and all CVE numbers: Excel, sheet "Vulnerabilities" (Schwachstellen).

Devices (22)

Devices with an insecure service are at the top (dot). All details per device - ports, versions, script output - are in the Excel file.

IP address	Device	Vendor	Name / model, firmware	Insecure services	Open ports
192.168.30.3	Network device	Cisco Systems	Cisco IOS Software, IE3x00 Software (IE3x00-UNIVERSALK9-M) FW...	HTTP, SNMP, Telnet	T:22,443,23,80 U:161
192.168.30.4	Network device	Hirschmann Automation and Control	Hirschmann Railswitch Power RSP35 HiOS-3S 08.7.02 FW 08.7.02	HTTP, SNMP, Telnet	T:23,80 U:161
192.168.30.20	Controller (PLC)	Schneider Electric	Modicon M340 CPU, Firmware V2.70 FW V2.70	FTP, HTTP, SNMP	T:21,80,502 U:161
192.168.30.30	Unknown device	Moxa Technologies	NPort 5150 Firmware 3.9 Build 20052616 FW 3.9	HTTP, SNMP, Telnet	T:23,80 U:161
192.168.30.31	Unknown device	Moxa Technologies	NPort 5150 Firmware 3.9 Build 20052616 FW 3.9	HTTP, SNMP, Telnet	T:23,80 U:161
192.168.30.102	Network device	Hirschmann Automation and Control	Hirschmann Automation and Control GmbH Hirschmann RSR	HTTP, SNMP, Telnet	T:23,80 U:161
192.168.30.22	Controller (PLC)	Wago Kontakttechnik	WAGO 750-8212 PFC200 G2 2ETH RS	FTP, HTTP	T:21,22,80,443,502,2455
192.168.30.25	Controller (PLC)	Siemens	SIMATIC HMI Miniweb	HTTP, VNC	T:80,5900,102
192.168.30.26	Controller (PLC)	Siemens	SIMATIC HMI Miniweb	HTTP, VNC	T:80,5900,102
192.168.30.60	PC / server	Fujitsu Technology Solutions	-	RPC, SMB	T:135,445,3389
192.168.30.61	PC / server	Fujitsu Technology Solutions	-	RPC, SMB	T:135,445
192.168.30.10	Controller (PLC)	Siemens	H3-MO-SPS-L1 · CPU 315-2 PN/DP FW 3.2.14	HTTP, SNMP	T:80,102 U:161,34964
192.168.30.11	Controller (PLC)	Siemens	H3-MO-SPS-L2 · CPU 317-2 PN/DP FW 3.2.15	HTTP, SNMP	T:80,102 U:161,34964
192.168.30.1	Network device	Fortinet	-	SNMP	T:443 U:161
192.168.30.2	Network device	Siemens	SCALANCE XC208 6GK5 208-0BA00-2AC2 FW V4.3	SNMP	T:22,443 U:161
192.168.30.15	Controller (PLC)	Siemens	H3-MO-SPS-ST01 · CPU 1214C DC/DC/DC FW 4.2.3	HTTP	T:102,80,443
192.168.30.16	Controller (PLC)	Siemens	H3-MO-SPS-ST02 · CPU 1215C DC/DC/DC FW 4.5.2	HTTP	T:102,80,443
192.168.30.21	Controller (PLC)	OMRON	-	HTTP	T:80,9600,44818 U:9600
192.168.30.101	Controller (PLC)	Siemens, Automations & Drives	SIMATIC HMI	HTTP	T:80,102,443
192.168.30.12	Controller (PLC)	Siemens	H3-MO-SPS-L3 · CPU 1516-3 PN/DP FW 2.9.4	-	T:102,443,4840
192.168.30.17	Controller (PLC)	Siemens	H3-MO-SPS-ST03 · CPU 1214C DC/DC/DC FW 4.4.1	-	T:102
192.168.30.100	Controller (PLC)	Siemens	-	-	T:102,4840

Firewall traffic and CMDB

Splunk 02.11.2026 - 08.11.2026: 2 devices are only visible in firewall traffic, not in the scan. New and affected CMDB rows are in the file "..._CMDB-Nachtrag.xlsx", the search help (MAC, location, partner) in the Excel sheet "Only in Splunk" (Nur in Splunk).

IP address	Assessment	In CMDB	Splunk ports	Last seen
192.168.30.90	Present - outbound only	no	-	2026-11-08
192.168.30.91	Present - outbound only	no	-	2026-11-08

CMDB (Musterwerk_Halle3_CMDB.xlsx): 19 entries in this network. 3 devices in the scan but not in the CMDB: 192.168.30.1, 192.168.30.17, 192.168.30.26. 0 CMDB entries were not found in the scan (list: Excel, sheet "CMDB-Ansicht").

Communication through the firewall

Splunk 02.11.2026 - 08.11.2026: 13 connection types with 7 partner zones. No permitted connection uses an insecure protocol. The complete list (all partners, ports, devices) is in the Excel sheet "Communication" (Kommunikation).

Direction	Partner zone / network	Port	Service	Devices	Connections	Note
incoming	Z-Produktion	TCP 102	S7	10	753.530	-
incoming	Z-Produktion	TCP 4840	OPC-UA	2	151.335	-
incoming	Z-Leitebene	TCP 502	MODBUS	2	98.695	-
outgoing	Z-Infrastruktur	UDP 123	NTP	21	30.158	-
outgoing	Z-Produktion	TCP 102	S7	1	22.140	-
incoming	Z-Leitebene	UDP 9600	OMRON-FINS	1	21.379	-
outgoing	Z-Leitebene	TCP 502	MODBUS	1	15.880	-
outgoing	Z-Infrastruktur	UDP 514	SYSLOG	3	9.745	-
outgoing	Z-Infrastruktur	TCP 443	HTTPS	2	2.452	-
incoming	Z-Engineering	TCP 102	S7	10	1.431	-
incoming	Z-DMZ	TCP 3389	RDP	1	61	-
incoming	Z-Engineering	TCP 5900	VNC	1	12	rejected only
incoming	Z-Engineering	TCP 21	FTP	1	6	rejected only

Key figures

Key figure	This scan	Last full scan
Traffic light	yellow	-
Devices found	22	-
Devices with insecure service	19	-
Insecure services	38	-
Model or firmware detected	17 (77 %)	-
of which with firmware version	12	-
Insecure services without firewall traffic	38	-
Only in firewall traffic (Splunk)	2	-
Devices found in CMDB	19 of 22	-
CMDB entries found in scan	19 of 19	-
Devices with vendor advisory (firmware affected)	9	-
Devices with vendor advisory (only model matches)	2	-
of which actively exploited vulnerability (KEV)	0	-
Permitted insecure connections through the firewall	0	-

To work through: "..._Massnahmen.xlsx" (insecure services and vendor advisories per device with location, priority and status column). For the CMDB: "..._CMDB-Delta.xlsx" (new / changed / missing).

About this scan

Item	Value
Network	Montage_Anlagennetz
Address range	192.168.30.0/24
Scan type	Staged scan complete
Port selection	ICS_OT_CORE
Start	10.11.2026 14:20
End	10.11.2026 15:48
Duration	1 h 28 min
Complete	yes
nmap version	7.94
Report created	13.11.2026 01:58

Assessment: every open port is checked against the traffic rules (HanselCraft default, based on IEC 62443). Non-permitted protocols with remote control or file access count 3, non-permitted ones with plain-text login 2, secondary ports and those permitted with TLS 1. A port scan does not show versions of login methods (e.g. SMBv1/v3, SNMPv1/v3); these must be checked on the device. The scan does not use attack, brute-force or vulnerability scripts.

Scan arguments (per stage, without target lists):

nmap -sS -sU -Pn -n -T2 --max-retries 3 --host-timeout 1800s --reason --open -sV --version-intensity 5 -O -p T:21,22,23,80,102,135,443,445,502,1200,2455,3389,4840,5900,8000,9600,44818,U:161,3671,9600,34964,47808 --script banner,http-server-header,http-title,ssl-cert,snmp-sysdescr,s7-info_robust,modbus-identity,codesys-v2-discover,knx-gateway-info,bacnet-info 192.168.30.0/24