OTScan 3

OT-/ICS-NETZWERKSCANNER · HANSELCRAFT

NETWORK CHECK

Montage_Anlagennetz

Scan 10.11.2026 14:20 – 10.11.2026 15:48 · Staged scan complete

YELLOW

DEVICES	INSECURE SERVICES	VENDOR ADVISORIES	STATUS
22	19 devices	11 devices	10.11.2026 15:48

1 At a glance

YELLOW

Assessment: 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.

What now? Agree on the actions with the people responsible for the plant and schedule them.

22 Devices in scan	**19** with insecure services	**19** of which no firewall traffic
11 with vendor advisory	**3** new for CMDB	**0** in CMDB, not found

KEY POINTS

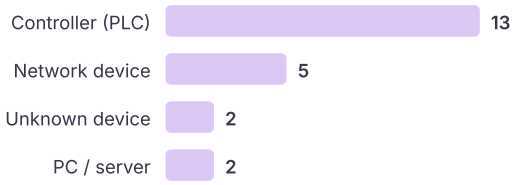
Info	22 devices were found in network Montage_Anlagennetz.
Attention	19 of 22 devices offer at least one insecure service.
Attention	9 devices are affected according to vendor advisories (firmware in the affected range); for 2 devices, the model matches an advisory – check the firmware on the device.
Attention	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.
Attention	38 of 38 insecure services had no traffic through the firewall during the Splunk period 02.11.2026 – 08.11.2026 - candidates for disabling.
Attention	Most common: HTTP on 15 devices, SNMP on 10 devices, Telnet on 5 devices.
Info	Most devices are: Controller (PLC) (13 of 22).

2 Network and devices

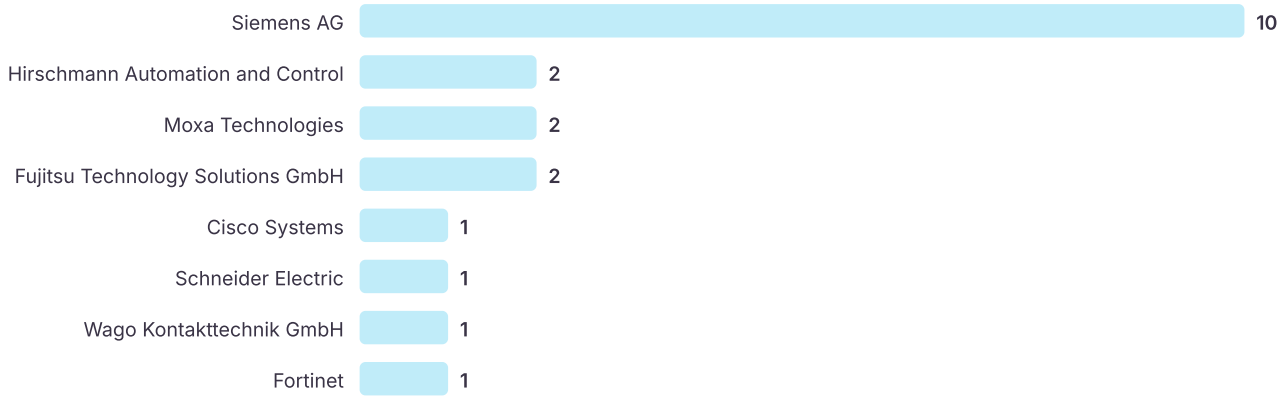
PROFILE

Network	Montage_Anlagennetz
Scan from – to	10.11.2026 14:20 – 10.11.2026 15:48
Duration	1 h 28 min
Complete?	Yes
Scan profile	Staged scan complete
Port selection	ICS_OT_CORE

DEVICE CLASSES

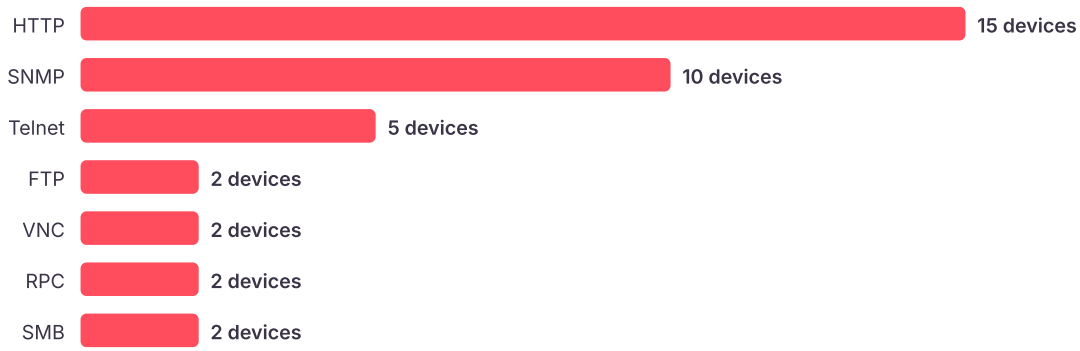


VENDOR



3 Insecure services

Services that are not permitted under the traffic rules or must be secured. Dark = share of devices without traffic through the firewall – candidates for disabling.



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".

17	99	17
Actions high	Actions medium	Actions low

Urgency = how quickly and easily something can be fixed, not the risk. List to tick off: "..._Massnahmen.xlsx".

4 Vendor advisories

Comparison of model and firmware with the vendor advisories. Quality "model" = model matches, check firmware on the device.

Advisory	Title	Model	CVSS	Quality	Devices
SSA-001536	SSA-001536: Authorization Bypass Vulnerability in Siemens Industrial Edge Devices	SIMATIC HMI	10.0	vendor	1
SEVD-2021-313-05	BadAlloc Vulnerabilities	Modicon M340 CPU, Firmware V2.70	9.8	model	1
SSA-941426	SSA-941426: Multiple LLDP Vulnerabilities in Industrial Products	SIMATIC HMI, Siemens TP1200 Comfort V16	9.8	model	2
SSA-478893	SSA-478893: TightVNC Vulnerabilities in Industrial Products (Revoked)	SIMATIC HMI	9.8	vendor	1
SSA-940818	SSA-940818: UltraVNC Vulnerabilities in SIMATIC HMIs/WinCC Products	SIMATIC HMI	9.8	vendor	1
SSA-538778	SSA-538778: SmartVNC Vulnerabilities in SIMATIC HMI/WinCC Products	SIMATIC HMI	9.8	vendor	1
SSA-452276	SSA-452276: Eval Injection Vulnerability in SIMATIC S7-1500	CPU 1516-3 PN/DP	9.6	exact	1
SSA-591731	SSA-591731: Multiple Vulnerabilities in SIMATIC S7 PLCs Web Server	CPU 1516-3 PN/DP	9.6	exact	1
SSA-699386	SSA-699386: Multiple Vulnerabilities in SCALANCE XB-200 / XC-200 / XP-200 / XF-200BA / XR-	SCALANCE XC208 6GK5 208-0BA00-2AC2	9.1	exact	1
SSA-710008	SSA-710008: Multiple Web Vulnerabilities in SCALANCE Products	SCALANCE XC208 6GK5 208-0BA00-2AC2	9.1	exact	1
SSA-832641	SSA-832641: Path Traversal Vulnerabilities in Siemens Industrial Edge Devices	SIMATIC HMI	9.1	vendor	1
SSA-688146	SSA-688146: Multiple Cross-Site Scripting Vulnerabilities in SIMATIC S7 PLCs Web Server	CPU 1516-3 PN/DP	9.1	exact	1
SSA-723487	SSA-723487: RADIUS Protocol Susceptible to Forgery Attacks (CVE-2024-3596) - Impact to SCA	SCALANCE XC208 6GK5 208-0BA00-2AC2	9.0	exact	1
SSA-552702	SSA-552702: Privilege Escalation Vulnerability in the Web Interface of SCALANCE and RUGGED	SCALANCE XC208 6GK5 208-0BA00-2AC2	8.8	exact	1
ICSA-19-346-02	Omron PLC CJ and CS Series	Omron NX1P2 1.40	8.6	model	1
SSA-328642	SSA-328642: "Copy Fail" Vulnerability in Multiple Industrial Products	SIMATIC HMI	7.8	vendor	1
SSA-387223	SSA-387223: Unauthenticated Control Panel Escape Vulnerability on SIMATIC HMI Unified Comf	SIMATIC HMI	7.7	vendor	1
SSA-712929	SSA-712929: Denial of Service Vulnerability in OpenSSL (CVE-2022-0778) Affecting Industria	CPU 1214C DC/DC/DC, CPU 1215C DC/DC/DC, CPU 1516-3	7.5	model	7

Advisory	Title	Model	CVSS	Quality	Devices
SSA-473245	SSA-473245: Denial of Service Vulnerability in Profinet Devices	CPU 315-2 PN/DP, CPU 317-2 PN/DP, SIMATIC HMI, Sie	7.5	model	4
SSA-711309	SSA-711309: Denial of Service Vulnerability in the OPC UA Implementations of SIMATIC Produ	CPU 1516-3 PN/DP, Siemens TP1200 Comfort V16	7.5	model	2
SSA-384224	SSA-384224: Denial of Service Vulnerability in SIMATIC HMI Panels	SIMATIC HMI, Siemens TP1200 Comfort V16	7.5	model	2
SSA-593272	SSA-593272: SegmentSmack in Interniche IP-Stack based Industrial Devices	CPU 315-2 PN/DP, CPU 317-2 PN/DP	7.5	exact	2
SSA-349422	SSA-349422: Denial of Service Vulnerability in Industrial Real-Time (IRT) Devices	CPU 315-2 PN/DP, CPU 317-2 PN/DP	7.5	exact	2
SSA-480230	SSA-480230: Denial of Service Vulnerability in Webserver of Industrial Products	CPU 315-2 PN/DP, CPU 317-2 PN/DP, SIMATIC HMI	7.5	exact	3
SSA-915282	SSA-915282: Denial of service Vulnerability in Interniche IP-Stack based Industrial Device	CPU 1214C DC/DC/DC, CPU 1516-3 PN/DP, CPU 315-2 PN	7.5	exact	4
SSA-392349	SSA-392349: Denial of Service Vulnerability in Industrial Devices	CPU 1516-3 PN/DP, CPU 315-2 PN/DP, CPU 317-2 PN/DP	7.5	exact	3
SSA-599968	SSA-599968: Denial of Service Vulnerability in Profinet Devices	CPU 1214C DC/DC/DC	7.5	exact	2
SSA-224824	SSA-224824: Denial of Service Vulnerabilities in SIMATIC S7-1200 CPU Family Before V4.7	CPU 1214C DC/DC/DC, CPU 1215C DC/DC/DC	7.5	exact	3
ICSA-18-317-08	Siemens SIMATIC Panels	SIMATIC HMI	7.5	model	1
SSA-307392	SSA-307392: Denial of Service in OPC UA in Industrial Products	SIMATIC HMI	7.5	vendor	1
SSA-592380	SSA-592380: Denial of Service Vulnerability in SIMATIC S7-1500 CPUs and related products	CPU 1516-3 PN/DP	7.5	exact	1
SSA-382653	SSA-382653: Multiple Denial of Service Vulnerabilities in Industrial Products	CPU 1516-3 PN/DP	7.5	exact	1
SSA-244969	SSA-244969: OpenSSL Vulnerability in Industrial Products	CPU 1214C DC/DC/DC	7.4	exact	2
SSA-264815	SSA-264815: Type Confusion Vulnerability in OpenSSL X.400 Address Processing in SIMATIC Pr	CPU 1516-3 PN/DP	7.4	exact	1
SSA-717113	SSA-717113: Cross-Site Request Forgery (CSRF) Vulnerability in SIMATIC S7-1200 CPUs before	CPU 1214C DC/DC/DC, CPU 1215C DC/DC/DC	7.1	exact	3
ICSA-15-099-01E	Siemens SIMATIC HMI Devices Vulnerabilities (Update E)	SIMATIC HMI	6.8	vendor	1
SEVD-2021-222-04	Modicon PAC Controllers and PLC Simulator for EcoStruxure™ Control Expert and EcoStruxure™	Modicon M340 CPU, Firmware V2.70	6.5	model	1
SSA-542525	SSA-542525: Authentication Vulnerabilities in SIMATIC HMI Products	SIMATIC HMI, Siemens TP1200 Comfort V16	6.5	model	2
SSA-285795	SSA-285795: Denial of Service in OPC-UA in Industrial Products	SIMATIC HMI, Siemens TP1200 Comfort V16	6.5	model	2
SSA-592007	SSA-592007: Denial of Service Vulnerability in Industrial Products	CPU 315-2 PN/DP, CPU 317-2 PN/DP	6.5	exact	2

Advisory	Title	Model	CVSS	Quality	Devices
SSA-478960	SSA-478960: Missing CSRF Protection in the Web Server Login Page of Industrial Controllers	CPU 1516-3 PN/DP, CPU 315-2 PN/DP, CPU 317-2 PN/DP	6.5	exact	3
SSA-413565	SSA-413565: Multiple Vulnerabilities in SCALANCE Products	SCALANCE XC208 6GK5 208-0BA00-2AC2	6.5	exact	1
SSA-293562	SSA-293562: Denial of Service Vulnerabilities in PROFINET DCP Implementation of Industrial	SIMATIC HMI	6.5	model	1
SSA-772220	SSA-772220: OpenSSL Vulnerabilities in Industrial Products	SIMATIC HMI, Siemens TP1200 Comfort V16	5.9	model	2
SSA-423808	SSA-423808: Multiple NULL Pointer Dereference Vulnerabilities in Industrial Products	SIMATIC HMI, Siemens TP1200 Comfort V16	5.9	model	2
SSA-264814	SSA-264814: Timing Based Side Channel Vulnerability in the OpenSSL RSA Decryption in SIMAT	CPU 1516-3 PN/DP, CPU 315-2 PN/DP, CPU 317-2 PN/DP	5.9	exact	3
SSA-179516	SSA-179516 OpenSSL Vulnerability in Industrial Products	SIMATIC HMI	5.9	model	1
ICSA-20-196-04	Siemens SIMATIC HMI Panels	SIMATIC HMI, Siemens TP1200 Comfort V16	5.7	model	2
SSA-446448	SSA-446448: Denial of Service Vulnerability in PROFINET Stack Integrated on Interniche Sta	CPU 315-2 PN/DP, CPU 317-2 PN/DP	5.3	exact	2
SSA-725549	SSA-725549: Denial of Service of ICMP in Industrial Devices	CPU 1214C DC/DC/DC, CPU 1516-3 PN/DP, CPU 315-2 PN	5.3	exact	4
SSA-195895	SSA-195895: User Enumeration Vulnerability in the Webserver of SIMATIC Products	CPU 1214C DC/DC/DC, CPU 1215C DC/DC/DC	5.3	exact	3
SSA-594364	SSA-594364: Denial-of-Service Vulnerability in SNMP Implementation of WinCC Runtime	SIMATIC HMI	5.3	model	1
SSA-054046	SSA-054046: Unauthenticated Information Disclosure in Web Server of SIMATIC S7-1500 CPUs	CPU 1516-3 PN/DP	5.3	exact	1
SSA-353002	SSA-353002: Multiple Vulnerabilities in SCALANCE XB-200 / XC-200 / XP-200 / XF-200BA / XR-	SCALANCE XC208 6GK5 208-0BA00-2AC2	4.9	exact	1
SSA-876787	SSA-876787: Open Redirect Vulnerability in SIMATIC S7-1500 and S7-1200 CPUs	CPU 1214C DC/DC/DC, CPU 1215C DC/DC/DC, CPU 1516-3	4.7	exact	4
ICSA-15-064-01	Siemens SIMATIC HMI Basic, SINUMERIK, and Ruggedcom APE GHOST Vulnerability	SIMATIC HMI	4.6	vendor	1
ICSA-15-064-01A	Siemens SIMATIC HMI Basic, SINUMERIK, and Ruggedcom APE GHOST Vulnerability (Update A)	SIMATIC HMI	4.6	vendor	1
SSA-482757	SSA-482757: Missing Immutable Root of Trust in S7-1500 CPU devices	CPU 1516-3 PN/DP	4.6	exact	1
ICSA-18-317-03	Siemens SIMATIC Panels and SIMATIC WinCC (TIA Portal)	SIMATIC HMI	4.3	model	1
SSA-273799	SSA-273799: Message Integrity Protection Bypass Vulnerability in SIMATIC Products	SIMATIC HMI	3.7	model	1

Advisory	Title	Model	CVSS	Quality	Devices
SESB-2019-214-01	Wind River VxWorks Vulnerabilities (URGENT/11)	Modicon M340 CPU, Firmware V2.70	0.0	model	1

5 Inventory and applications

Every device from CMDB, scan and firewall traffic (Splunk) – merged via IP, otherwise MAC.



confirmed (all sources) **19** new for CMDB **3** traffic only, unknown **2**

APPLICATIONS IN FIREWALL TRAFFIC

Communication partners assigned via the documentation database.

Application / system	Zone	Connections
MES Produktionsdaten	Z-Produktion	927.005
Prozessleitsystem	Z-Leitebene	135.954
Zeitdienst und Protokollierung	Z-Infrastruktur	42.355
MES Produktionsdaten	Z-Engineering	1.449
Fernwartung	Z-DMZ	61

TO BE CLARIFIED (5)

Status	IP address	Name	Type	Vendor	Note
new for CMDB	192.168.30.1	–	Network device	Fortinet	insecure services without firewall traffic – consider disabling
new for CMDB	192.168.30.17	–	Controller (PLC)	Siemens AG	
new for CMDB	192.168.30.26	–	Controller (PLC)	Siemens AG	insecure services without firewall traffic – consider disabling
traffic only, unknown	192.168.30.90	–	–	Siemens AG	
traffic only, unknown	192.168.30.91	–	–	Wago Kontakttechnik GmbH	

A Appendix: urgent actions (extract)

No.	IP address	CMDB name	Device	What	Recommendation
1	192.168.30.2	H3-MO-SW-01	Network device	SSA-699386: Multiple Vulnerabilities in SCALANCE XB-200 / XC-200 / XP-200 / XF-200BA / XR-300WG Family before V4.5	Update to V4.5 or later version
2	192.168.30.2	H3-MO-SW-01	Network device	SSA-710008: Multiple Web Vulnerabilities in SCALANCE Products	Update to V4.4 or later version
3	192.168.30.2	H3-MO-SW-01	Network device	SSA-723487: RADIUS Protocol Susceptible to Forgery Attacks (CVE-2024-3596) - Impact to SCALANCE, RUGGEDCOM and Related P	Update to V4.6 or later version
4	192.168.30.3	H3-MO-SW-02	Network device	Telnet (TCP 23)	Not permitted under the traffic rules: disable, use SSH for remote access.
5	192.168.30.4	H3-MO-SW-03	Network device	Telnet (TCP 23)	Not permitted under the traffic rules: disable, use SSH for remote access.
6	192.168.30.12	H3-MO-SPS-L3	Controller (PLC)	SSA-452276: Eval Injection Vulnerability in SIMATIC S7-1500	Update to V2.9.9 or later version
7	192.168.30.12	H3-MO-SPS-L3	Controller (PLC)	SSA-591731: Multiple Vulnerabilities in SIMATIC S7 PLCs Web Server	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
8	192.168.30.12	H3-MO-SPS-L3	Controller (PLC)	SSA-688146: Multiple Cross-Site Scripting Vulnerabilities in SIMATIC S7 PLCs Web Server	Restrict TIA project download to trusted personnel only.
9	192.168.30.20	H3-MO-SPS-FT	Controller (PLC)	FTP (TCP 21)	Not permitted under the traffic rules: disable, otherwise use SFTP or FTPS.
10	192.168.30.22	H3-MO-AS-01	Controller (PLC)	FTP (TCP 21)	Not permitted under the traffic rules: disable, otherwise use SFTP or FTPS.
11	192.168.30.25	H3-MO-HMI-01	Controller (PLC)	VNC (TCP 5900)	Not permitted under the traffic rules: disable or use only encrypted (TLS, VPN, SSH tunnel).
12	192.168.30.26	–	Controller (PLC)	VNC (TCP 5900)	Not permitted under the traffic rules: disable or use only encrypted (TLS, VPN, SSH tunnel).
13	192.168.30.30	H3-MO-GW-01	Unknown device	Telnet (TCP 23)	Not permitted under the traffic rules: disable, use SSH for remote access.
14	192.168.30.31	H3-MO-GW-02	Unknown device	Telnet (TCP 23)	Not permitted under the traffic rules: disable, use SSH for remote access.
15	192.168.30.60	H3-MO-ENG-01	PC / server	SMB (TCP 445)	Disable SMBv1 (not permitted under the traffic rules), use SMBv3 with signing, restrict access.
16	192.168.30.61	H3-MO-BED-01	PC / server	SMB (TCP 445)	Disable SMBv1 (not permitted under the traffic rules), use SMBv3 with signing, restrict access.
17	192.168.30.102	H3-MO-GER-52	Network device	Telnet (TCP 23)	Not permitted under the traffic rules: disable, use SSH for remote access.

B Terms

CMDB	Inventory (CMDB): the self-maintained device list as Excel (template from OTScan 3 or your own list). Provides name, type, vendor, location, trade and responsible persons. OTScan 3 only reads it.
Overall inventory	One Excel file with all devices from CMDB, scan and Splunk – each value with its source. Basis for the initial inventory.
Documentation database	Applications, servers, zones and network areas from the network and application overview and the research register. OTScan 3 uses it to assign communication partners to applications.
Scan / staged scan	Active detection by OTScan 3 in stages (reachability, services, device details).
Splunk	Analysis of the firewall logs: addresses, partners, ports, zones. Traffic within a network is not visible there.
Traffic light	GREEN = no insecure services. YELLOW = insecure services – close in a planned way. RED = particularly dangerous services – clarify immediately.
Insecure service	Service that the traffic rules (HanselCraft default, customizable) prohibit or only allow when secured (e.g. FTP, Telnet, HTTP login, SNMPv1/v2c).
Without firewall traffic	The service was not used through the firewall during the Splunk period – candidate for disabling.
Vendor advisory	Security advisory from a vendor (CSAF, CISA ICS). Quality exact / model / vendor.
Zone / service / policy	From the FortiGate log: security zone of source and destination, service name, firewall rule number.
Risk (detail view)	2 points per critical port (max. 8), +2 for a vendor advisory with CVSS ≥ 7, +1 for a weaker advisory.