CLAROTY
Clarity for OT Networks

Risk Assessment Report

SolutionsPT

July 06, 2020

NETWORK HYGIENE SCORE **69%**

ⓘ *The calculation represented in the Hygiene Score indicates the cumulative risk level the alerts, insights, and assets pose to the system. A low value means your system is more vulnerable to attacks.*

KEY FINDINGS

- ❗ 11 security alerts have been detected
- ❗ 52 process integrity alerts have been detected
- 💡 17 assets were communicating with 13 external IPs (9 of them are ghost)
- 💡 1 asset has 56 unpatched vulnerabilities - Full Match
- 💡 44 assets are using 4 unsecured protocols: FTP, SMTP, SSL, TELNET
- 💡 Top 3 Risky Assets
- 💡 6 assets using IT protocols: LDAPS, NETBIOS-NAME, POP3,... , with 4 PLCs/Controllers/RTUs/IEDs
- 💡 3 assets have multiple network interfaces
- 💡 2 OT-assets performed privileged OT operations on 2 PLCs/Controllers/RTUs/IEDs
- 💡 3 assets managed 6 assets remotely using protocols: SSH, TELNET
- 💡 4 OT-assets performed data-acquisition write operations on 2 PLCs/Controllers/RTUs/IEDs

TABLE OF CONTENTS

OVERVIEW

This report summarizes findings generated by Continuous Threat Detection (CTD) solution from an automated assessment of your operational network. This point in time assessment provides visibility into the assets on the network, how the assets are configured, the protocols being used and how the assets are communicating. The findings include insights into network hygiene and vulnerable assets (CVEs) that provide attack pathways or may cause network issues that can disrupt your operational processes. The report also summarizes threats found in your network.

CTD has identified assets from various types, including controllers, workstations, servers and networking infrastructure, communicating over a wide range of OT and IT protocols. A summary of the assets and details about assets are provided below. The communication details, summarized in various graphs below, can provide the security and operations teams a better understanding of the network and assist in identifying possible configuration issues.

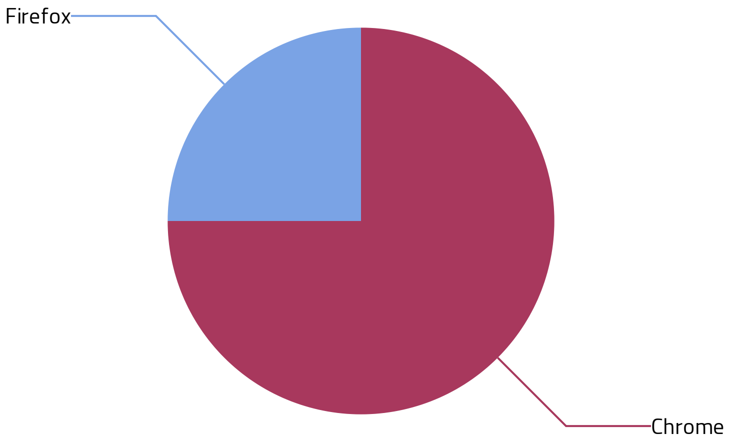
COUNTERS

24	19	52	0	39
Vendors	OT Assets	IT Assets	IoT Assets	Protocols

ASSET DISTRIBUTION BY INSTALLED PROGRAMS

CHROME:
75.0 %

FIREFOX:
25.0 %



ASSET DISTRIBUTION BY TYPE

ENDPOINT:

70.4 %

PLC:

9.9 %

OT:

7.0 %

HMI:

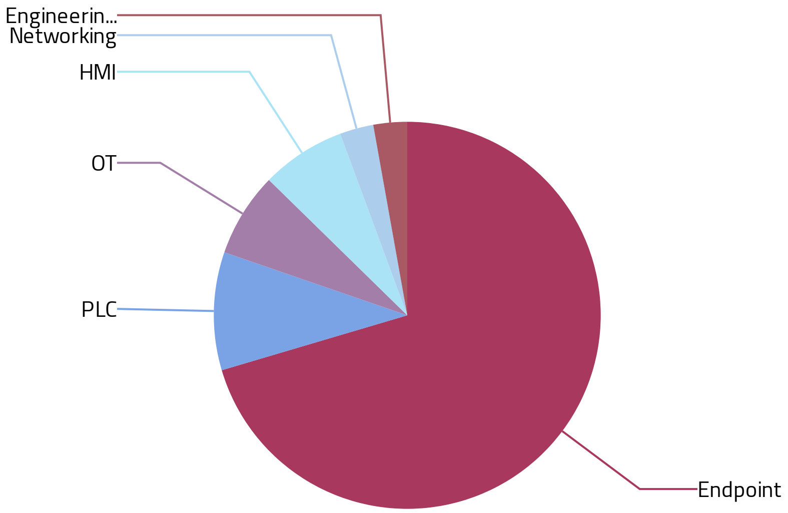
7.0 %

NETWORKING:

2.8 %

ENGINEERING STATION:

2.8 %



ASSET VENDORS

PHOENIX CONTACT ELECTRONICS:
27.0 %

VMWARE:
12.7 %

SIEMENS:
11.1 %

APPLE:
4.8 %

HOST ENGINEERING:
4.8 %

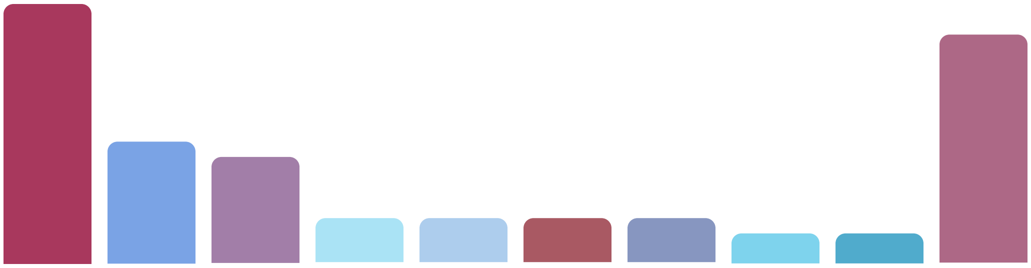
MOXA TECHNOLOGIES:
4.8 %

WISTRON INFOCOMMCO.LTD:
4.8 %

ADVANTECH:
3.2 %

ICPDAS:
3.2 %

OTHER:
23.8 %



ASSETS DISTRIBUTION BY FAMILY TYPE

OT:

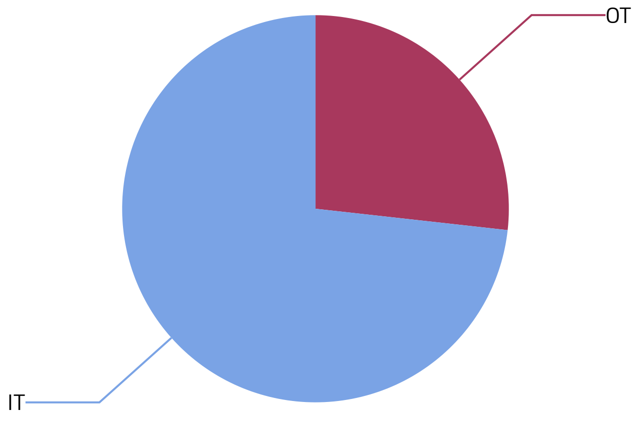
26.8 %

IT:

73.2 %

IOT:

0.0 %



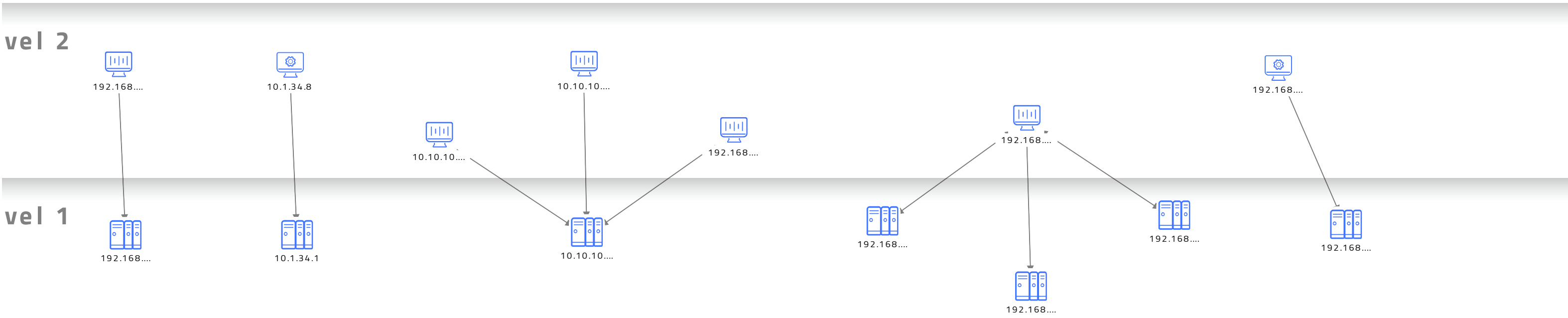
PROTOCOL TRAFFIC

No results found.

TOP VOLUME ASSETS

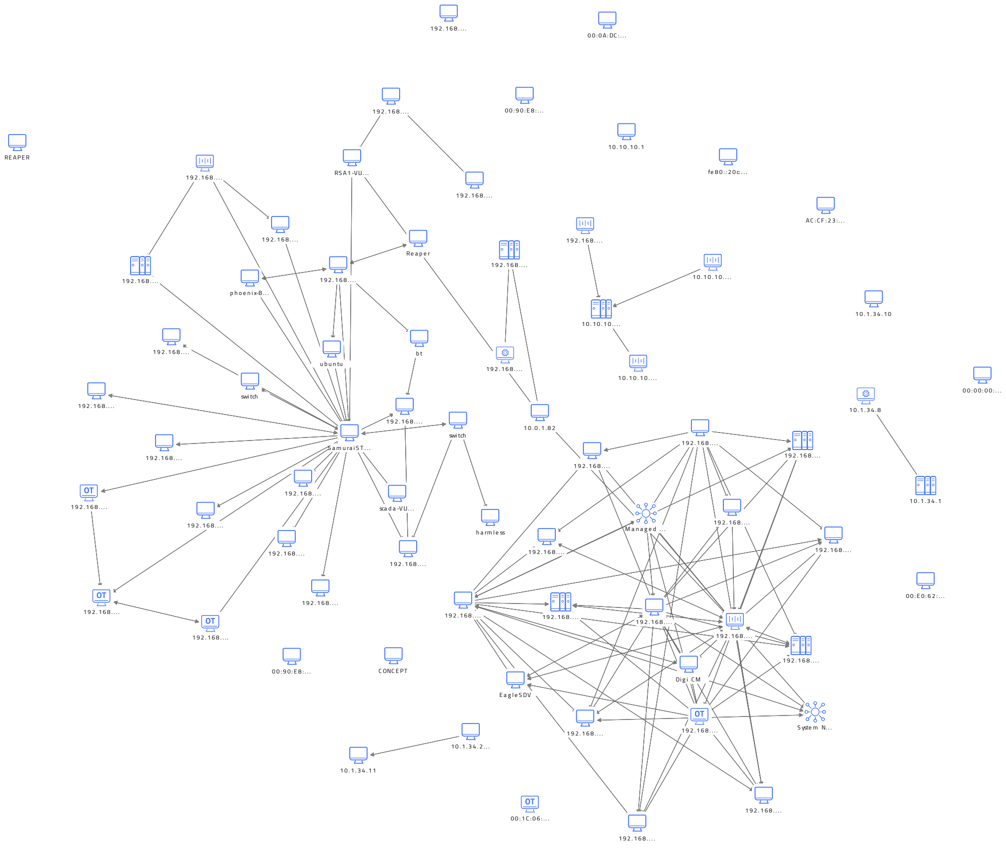
No results found.

OT GRAPH


vel 2
192.168....
10.1.34.8
10.10.10....
10.10.10....
192.168....
192.168....
192.168....
vel 1
192.168....
10.1.34.1
10.10.10....
192.168....
192.168....
192.168....
192.168....

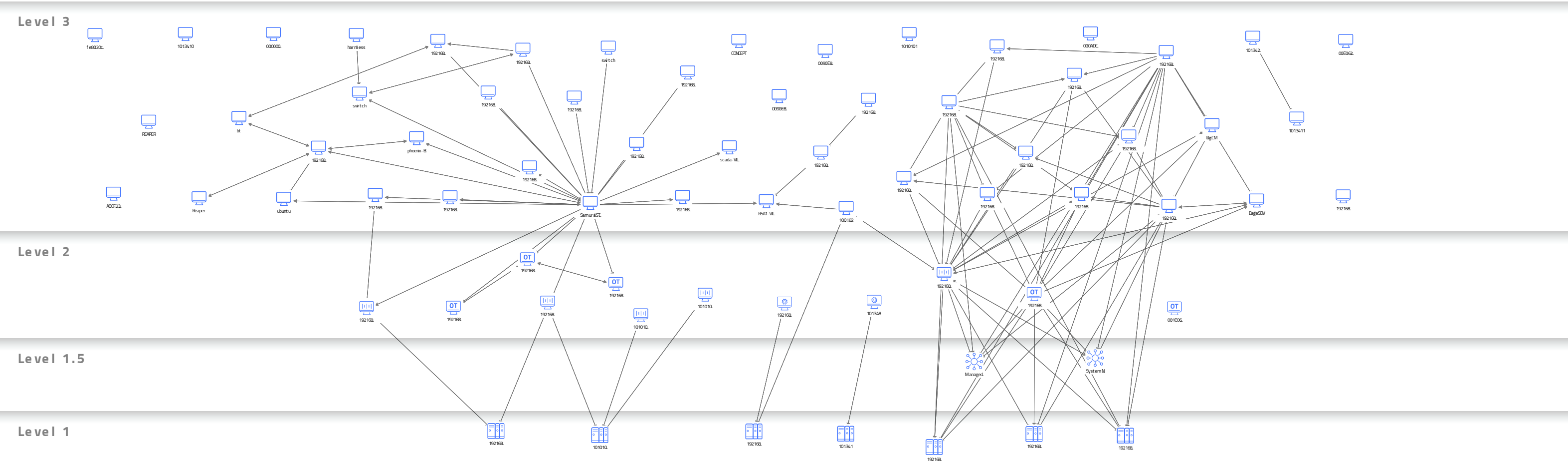
NETWORK COMMUNICATIONS

From the communication captured, different network maps were produced of the control traffic within the Site. The following diagram shows sample of filtered communication paths within the monitored networks.



LAYERED GRAPH

An additional way to display the communication paths is to associate the assets to the relative levels of the Purdue model.


Level 3
Level 2
Level 1.5
Level 1
fe8020c..
1013410
000000..
harmless
192168..
192168..
switch
CONCEPT
0090E8..
1010101
192168..
000ADE..
192168..
101342..
00E062..
REAPER
bt
switch
192168..
192168..
192168..
0090E8..
192168..
192168..
DigiCM
1013411
192168..
phoenix-B
192168..
192168..
scada-VIL
192168..
192168..
192168..
ACCF23..
Reaper
ubuntu
192168..
192168..
SamuraiST..
192168..
RSA1-VIL
100182
192168..
192168..
192168..
EagleSDV
192168..
192168..
192168..
192168..
192168..
192168..
192168..
101010..
101010..
192168..
101348
192168..
001C06..
Managed..
System N
192168..
101010..
192168..
101341
192168..
192168..
192168..

ALERTS

SECURITY ALERTS

Type	Description	Date Detected
Known Threat Alert	Known Threat: Threat VXWORKS-OS - Use of Urgent Flag might indicate potential attempt to exploit an Urgent11 RCE vulnerability was detected from 192.168.2.133 to 192.168.88.15	Mon Jul 06 2020
Known Threat Alert	Known Threat: Threat VXWORKS-OS Illegal use of Urgent pointer - Potential attempt to exploit an Urgent11 RCE vulnerability was detected from 192.168.2.133 to 192.168.88.20	Mon Jul 06 2020
Known Threat Alert	Known Threat: Threat VXWORKS-OS - Use of Urgent Flag might indicate potential attempt to exploit an Urgent11 RCE vulnerability was detected from 192.168.2.166 to 192.168.88.15	Mon Jul 06 2020
Known Threat Alert	Known Threat: Threat VXWORKS-OS Illegal use of Urgent pointer - Potential attempt to exploit an Urgent11 RCE vulnerability was detected from 192.168.2.166 to 192.168.88.20	Mon Jul 06 2020
Known Threat Alert	Known Threat: Threat VXWORKS-OS Illegal use of Urgent pointer - Potential attempt to exploit an Urgent11 RCE vulnerability was detected from 192.168.2.42 to 192.168.88.115	Mon Jul 06 2020
Known Threat Alert	Known Threat: Threat VXWORKS-OS - Use of Urgent Flag might indicate potential attempt to exploit an Urgent11 RCE vulnerability was detected from 192.168.2.42 to 192.168.88.115	Mon Jul 06 2020
Known Threat Alert	Known Threat: Threat Wannacry - IPC request to 192.168.56.20 (Hardcoded wannacry ip) detected was detected from 192.168.116.172 to 192.168.116.149	Mon Jul 06 2020
Suspicious File Transfer Alert	Suspicious file transfer found! File 'program 3' was transferred via 'TRISTATION' and matched the following Yara rules:	Mon Jul 06 2020

	['triton_claroty.yara/triton_download_payload'], Transferred from 192.168.1.88	
Suspicious File Transfer Alert	Suspicious file transfer found! File 'program 3' was transferred via 'TRISTATION' and matched the following Yara rules: ['ics_cert_hatman.yara/hatman_combined', 'ics_cert_hatman.yara/hatman'], Transferred from 192.168.1.88	Mon Jul 06 2020
Known Threat Alert	Out of working hours Known Threat: Threat Wannacry - IPC request to 192.168.56.20 (Hardcoded wannacry ip) detected was detected from 192.168.116.172 to 192.168.116.149	Mon Jul 06 2020
Suspicious Activity	Suspicious activity on controller **192.168.1.2** by **192.168.1.88**	Mon Jul 06 2020

INTEGRITY ALERTS

Type	Description	Date Detected
New Asset	New asset detected out of working hours : A new Endpoint was detected in vulnerable IT protocols permitted zone: "Endpoint: Other", performing network operation communication: 00a045606535	Mon Jul 06 2020
New Asset	New asset detected out of working hours : A new Endpoint was detected in vulnerable IT protocols permitted zone: "Endpoint: Other", performing network operation communication: 00a045606495	Mon Jul 06 2020
New Asset	New asset detected out of working hours : A new Endpoint was detected in vulnerable IT protocols permitted zone: "Endpoint: Other", performing network operation communication: 00a045697ebf	Mon Jul 06 2020
New Asset	New asset detected out of working hours : A new Endpoint was detected in vulnerable IT protocols permitted zone: "Endpoint: Other", performing network operation communication: 00a045697e7f	Mon Jul 06 2020
New Asset	New asset detected out of working hours : A new Endpoint was detected in vulnerable IT protocols permitted zone:	Mon Jul 06 2020

	"Endpoint: Other", performing network operation communication: 00a04560652b	
New Asset	New asset detected out of working hours : A new Endpoint was detected in vulnerable IT protocols permitted zone: "Endpoint: Other", performing network operation communication: 00a04537522c	Mon Jul 06 2020
New Asset	New asset detected out of working hours : A new Endpoint was detected in vulnerable IT protocols permitted zone: "Endpoint: Other", performing network operation communication: 00a0456064ef	Mon Jul 06 2020
New Asset	New asset detected out of working hours : A new Endpoint was detected in vulnerable IT protocols permitted zone: "Endpoint: Other", performing network operation communication: 00a0456064f9	Mon Jul 06 2020
New Asset	New asset detected out of working hours : A new Endpoint was detected in vulnerable IT protocols permitted zone: "Endpoint: Other", performing network operation communication: 192.168.0.42	Mon Jul 06 2020
Policy Violation Alert	Out of working hours Policy Violation: New non-risky protocol communication was detected from d4bed94b1258 to ffffffffffff	Mon Jul 06 2020
Policy Violation Alert	Out of working hours Policy Violation: New unclassified operation communication ports were detected from 192.168.0.109 to 192.168.0.107	Mon Jul 06 2020
Policy Violation Alert	Out of working hours Policy Violation: New non-risky protocol communication was detected from 192.168.0.1 to 192.168.0.107	Mon Jul 06 2020
New Asset	New asset detected out of working hours : A new Endpoint was detected in usage of Discovery protocols permitted zone: "Endpoint: Other - External", performing unclassified operation communication: 8.8.4.4	Mon Jul 06 2020
New Asset	New asset detected out of working hours : A new Endpoint was detected in vulnerable IT protocols permitted zone: "Endpoint: Other", performing	Mon Jul 06 2020

	unclassified operation communication: 192.168.1.1	
New Asset	New asset detected out of working hours : A new Endpoint was detected in vulnerable IT protocols permitted zone: "Endpoint: Other", performing network operation communication: fe80::ccd3:15de:cf75:5e28	Mon Jul 06 2020
New Asset	New asset detected out of working hours : A new Endpoint was detected in vulnerable IT protocols permitted zone: "Endpoint: Other", performing unclassified operation communication: fe80::92e6:baff:fe6c:b8e1	Mon Jul 06 2020
New Asset	New asset detected out of working hours : A new Endpoint was detected in vulnerable IT protocols permitted zone: "Endpoint: Other", performing network operation communication: 000000000000	Mon Jul 06 2020
Policy Violation Alert	Out of working hours Policy Violation: New non-risky protocol communication was detected from 192.168.0.109 to 192.168.0.107	Mon Jul 06 2020
Policy Violation Alert	Policy violation has been detected! Originated by 192.168.0.107	Mon Jul 06 2020
New Asset	New asset detected out of working hours : A new Endpoint was detected in vulnerable IT protocols permitted zone: "Endpoint: Other - External", performing unclassified operation communication: 192.160.0.20	Mon Jul 06 2020
Policy Violation Alert	Policy violation has been detected! Originated by 192.168.0.109	Mon Jul 06 2020
New Asset	New asset detected out of working hours : A new Endpoint was detected in vulnerable IT protocols permitted zone: "Endpoint: Other - External", performing unclassified operation communication: 10.0.0.1	Mon Jul 06 2020
Policy Violation Alert	Out of working hours Policy Violation: New protocol operation communication parameters were detected from 192.168.0.107 to 239.255.255.250	Mon Jul 06 2020
Policy Violation Alert	Out of working hours Policy Violation: New non-risky protocol communication was detected from 192.168.0.3 to 192.168.0.255	Mon Jul 06 2020
Policy Violation Alert	Out of working hours Policy Violation:	Mon Jul 06 2020

New non-risky protocol communication was detected from 192.168.0.103 to 192.168.0.255

INSIGHTS

UNSECURED PROTOCOLS

Protocols containing security weaknesses that attackers can leverage to compromise the network's security.

Protocol	Reason Protocol Is Unsecured	Assets Using This Protocol
TELNET	This protocol transfers data and credentials in a plain-text manner.	41 assets
FTP	This protocol transfers data and credentials in a plain-text manner.	36 assets
SMTP	This protocol transfers data and credentials in a plain-text manner.	34 assets
SSL	SSL/TLS of early version have been deprecated and considered unsecure due to weak cipher keys that can be recoverable and therefore can lead to deciphering of the encrypted channels.	14 assets

TOP RISKY ASSETS

Assets with the highest risk score
The Risk Score indicates the risk level of an asset. The higher the score, the riskier the asset.

Asset	Type	Risk score
192.168.2.133	HMI	71
SamuraiSTFU	Endpoint	69
Managed Redundant Switch 04759	Networking	62

PLCS TALKING IT PROTOCOL

Asset is communicating using IT protocol. This could be the result of misconfiguration or malicious activity.

Talking Asset	Protocol	PLC/Controller/RTU
192.168.2.133	RDP	3 assets
192.168.2.133	SSL	3 assets
192.168.2.133	POP3	3 assets
192.168.2.133	PORTMAPPER	3 assets
192.168.2.137	LDAPS	3 assets
192.168.2.133	SMTP	3 assets
192.168.2.137	NETBIOS-NAME	3 assets
192.168.2.133	NETBIOS-NAME	3 assets
192.168.2.137	RDP	3 assets
192.168.2.137	WHOIS	3 assets
192.168.2.137	RLOGIN	3 assets
192.168.2.137	POP3	3 assets
192.168.2.137	SMTP	3 assets
192.168.2.133	RLOGIN	3 assets
192.168.2.137	SSL	3 assets
192.168.2.137	PORTMAPPER	3 assets
192.168.2.137	TACACS	3 assets
192.168.2.133	LDAPS	3 assets
192.168.2.137	TDS	3 assets
192.168.2.133	TACACS	3 assets

TALKING WITH EXTERNAL IPS

External IPs, with respective network interfaces expose the asset to users outside of the company's perimeter, enabling attackers to enter the OT network.

Name	External IP	Is Ghost	Talked By
Managed Redundant Switch 09404	192.168.88.61	False	5 assets
8.8.8.8	8.8.8.8	True	3 assets
X	192.168.0.107	False	2 assets
192.160.0.20	192.160.0.20	True	2 assets
17.253.34.253	17.253.34.253	True	2 assets
WIN-U9C5BE8KCJV	192.168.0.2	False	2 assets
8.8.4.4	8.8.4.4	True	2 assets
192.168.0.99	192.168.0.99	False	1 asset
10.0.0.1	10.0.0.1	True	1 asset
192.168.86.1	192.168.86.1	True	1 asset
192.195.142.13	192.195.142.13	True	1 asset
10.1.0.132	10.1.0.132	True	1 asset
127.0.0.1	127.0.0.1	True	1 asset

MULTIPLE INTERFACES

Every network interface enables independent communication. This may compromise the efficiency of firewall segmentation, which might not take into consideration all the networking interfaces, when defining the asset's policy.

Name	Number of Interfaces
ubuntu	2
192.168.0.32	2
192.168.0.33	2

PRIVILEGED OPERATIONS (OPERATED PLCS)

Privileged commands are commands that are not part of the standard data acquisition commands. These commands are often used as part of engineering work such as configuration download/upload, or changing settings and modes.

OT-Asset	Type	Protocol	Operated On
192.168.1.88	Engineering Station	TRISTATION	1 PLC
10.1.34.8	Engineering Station	FTP	1 PLC
10.1.34.8	Engineering Station	MODBUS	1 PLC

CLIENTS REMOTELY MANAGED

Assets feature a connection with remote users (3rd parties or employees) for various maintenance purposes.

Managing Asset	Managing Protocol	Managed Assets
192.168.2.137	SSH	4 assets
192.168.2.133	SSH	4 assets
192.168.2.137	TELNET	3 assets
192.168.2.64	SSH	3 assets
192.168.2.133	TELNET	3 assets
192.168.2.64	TELNET	2 assets

TALKING WITH GHOST ASSETS

Ghost assets are network entities that never replied. These assets could be the result of a misconfiguration and can be used as an attack surface into the network. Attackers can hijack such communication by impersonating a ghost asset, compromising the talking asset.

Ghost Asset	Protocol	Talked By
192.168.88.2	SSL	4 assets
192.168.88.80	SSL	3 assets
192.168.88.85	SSL	3 assets
192.168.88.2	HTTP	3 assets
192.168.88.85	ICMP	2 assets
192.168.88.85	TCP	2 assets
192.168.88.80	HTTP	2 assets
192.168.88.85	HTTP	2 assets
192.168.88.2	TCP	2 assets
192.168.88.85	NETBIOS-NAME	1 asset
192.168.88.85	POP3	1 asset
192.168.88.85	PORTMAPPER	1 asset
192.168.88.85	RDP	1 asset
192.168.88.85	RPC	1 asset
192.168.88.85	SMTP	1 asset
192.168.88.85	SSH	1 asset
192.168.88.85	TELNET	1 asset
192.168.88.2	FTP	1 asset
192.168.88.2	ICMP	1 asset
192.168.88.2	LDAPS	1 asset

DATA ACQUISITION WRITE (OPERATED PLCS)

This insight includes all the assets that performed data acquisition write actions. These assets should be considered as potential assets that can change the process by changing values.

Writing OT-Asset	Type	Protocol	Operated On
10.10.10.20	HMI	S7COMM	1 asset
10.10.10.30	HMI	S7COMM	1 asset
192.168.1.10	HMI	S7COMM	1 asset
192.168.2.133	HMI	MODBUS	1 asset

DHCP CLIENTS

A DHCP server enables clients to request IP addresses and networking parameters automatically. It's important to monitor the DHCP servers in the network because an attacker can pretend to be the server and use it to perform various attacks.

Server	Protocol	Clients
192.168.0.100	DHCPv4	5 clients

ASSETS THAT HIGHLY CONNECTED ASSETS TALKED TO

These assets are highly ranked in terms of the amount of network connections they initiate. In some cases, this indicates key elements in the network such as data collection services, monitor servers, or possibly an adversary performing broad reconnaissance.

Asset	Type	Protocol	Neighbors
SamuraiSTFU	Endpoint	HTTP	22 assets
SamuraiSTFU	Endpoint	SSL	21 assets
SamuraiSTFU	Endpoint	TCP	20 assets
SamuraiSTFU	Endpoint	RPC	20 assets
SamuraiSTFU	Endpoint	TELNET	19 assets
SamuraiSTFU	Endpoint	POP3	19 assets
SamuraiSTFU	Endpoint	PORTMAPPER	19 assets
SamuraiSTFU	Endpoint	RDP	18 assets
192.168.2.133	Endpoint	ICMP	14 assets
192.168.2.133	Endpoint	SSL	14 assets
192.168.2.137	Endpoint	HTTP	13 assets
192.168.2.137	Endpoint	SSL	13 assets
192.168.2.44	Endpoint	TCP	12 assets

WEB CLIENTS

Assets that function as web servers.

Server	URL	Accessed Clients
Managed Redundant Switch 04759	192.168.88.60/	5 assets
Digi CM	192.168.88.115/	3 assets
192.168.88.100	192.168.88.100/	3 assets
Managed Redundant Switch 09404	192.168.88.61/	3 assets
192.168.88.20	192.168.88.20/	3 assets
System Name	192.168.88.95/	2 assets
192.168.88.51	192.168.88.51/	2 assets
Managed Redundant Switch 04759	192.168.88.60/auth/	2 assets
192.168.88.49	192.168.88.49/	2 assets
Managed Redundant Switch 04759	192.168.88.60/favicon.ico	2 assets
192.168.0.1	192.168.0.1/	2 assets
192.168.88.25	192.168.88.25/favicon.ico	1 asset
192.168.88.25	192.168.88.25:81/	1 asset
192.168.88.25	192.168.88.25/	1 asset
192.168.88.51	192.168.88.51/sra_{BA195980-CD49-458b-9E23-C84EE0ADCD75}	1 asset
192.168.0.1	192.168.0.1/14.gif	1 asset
192.168.0.1	192.168.0.1/13.gif	1 asset
192.168.0.1	192.168.0.1/12.gif	1 asset
192.168.0.1	192.168.0.1/11.gif	1 asset
System Name	192.168.88.95/sra_{BA195980-CD49-458b-9E23-C84EE0ADCD75}	1 asset

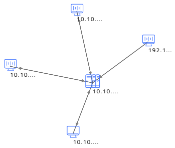
ASSETS

ASSET INFORMATION

Asset Name	Type	Site	Vendor
10.10.10.10	PLC	SolutionsPT	Siemens

IP	MAC	Protocols
10.10.10.10	28:63:36:89:59:82	ARP, S7COMM, TCP

NETWORK COMMUNICATIONS



VENDOR MATCH CVES

This table lists assets that run vulnerable software versions and can be leveraged by attackers for various malicious purposes such as, remote code execution, DDOS, etc.

Vulnerabilities are matched against these assets' vendor name

<table>
<tr><th>CVE-ID</th><th>SCORE (CVSS)</th><th>TITLE</th><th>PUBLISHED</th><th>MODIFIED</th><th>IDENTIFIED ON</th></tr>
<tr><td>SSA-902727</td><td><b>10.0</b></td><td>Multiple Vulnerabilities in Licensing Software for SISHIP Automation</td><td>14/05/19 01:00</td><td>14/05/19 01:00</td><td>06/07/20 16:38</td></tr>
<tr><td colspan="6">Access Type: Network
Multiple vulnerabilities have been identified in the WibuKey Digital Rights Management (DRM) solution, which affect SISHIP Automation Solutions. Siemens recommends users to apply the updates to WibuKey Digital Rights Management (DRM) provided by WIBU SYSTEMS AG.
Related CVEs: CVE-2018-3989, CVE-2018-3990, CVE-2018-3991
Link 1</td></tr>
<tr><td>CVE-2016-7112</td><td><b>10.0</b></td><td>Authentication Bypass Vulnerability in SIPROTEC</td><td>09/05/16 01:00</td><td>22/03/18 00:00</td><td>06/07/20 16:38</td></tr>
<tr><td colspan="6">Access Type: Network
Attackers with network access to the device’s web interface (Port 80/TCP) could circumvent authentication and perform certain administrative operations.
Related CVEs: SSA-630413 , ICSA-17-187-03
Link 1</td></tr>
<tr><td>ICSA-16-040-02</td><td><b>10.0</b></td><td>Denial-of-service condition or a replay attack</td><td>22/03/16 00:00</td><td>22/03/16 00:00</td><td>06/07/20 16:38</td></tr>
</table>

CVE-ID	SCORE (CVSS)	TITLE	PUBLISHED	MODIFIED	IDENTIFIED ON	
Access Type: Unknown Successful exploitation of these vulnerabilities could result in a denial-of-service condition or a replay attack on the affected devices Related CVEs: Link 1						
SSA-982399	**10.0**	Missing Authentication in TIM 1531 IRC Modules	11/12/18 00:00	17/12/18 00:00	06/07/20 16:38	^
Access Type: Network The latest update for TIM 1531 IRC fixes a vulnerability. The devices was missing proper authentication when connecting on port 102/tcp, although configured. An attacker needs to be able to connect to port 102/tcp of an affected device in order to exploit this vulnerability. The vulnerability could allow an attacker to perform administrative operations. Siemens has released updates for TIM 1531 IRC modules. Related CVEs: CVE-2018-13816 Link 1						
SSA-170881	**10.0**	Vulnerabilities in SINUMERIK Controllers	11/12/18 00:00	12/03/19 00:00	06/07/20 16:38	^

CVE-ID	SCORE (CVSS)	TITLE	PUBLISHED	MODIFIED	IDENTIFIED ON

Access Type: Network

The latest updates for SINUMERIK controllers fix multiple security vulnerabilities that could allow an attacker to cause Denial-of-Service conditions, escalate privileges, or to execute code from remote. Siemens has released updates for several affected products, is working on updates for the remaining affected products and recommends specific countermeasures until fixes are available. Siemens recommends to update affected devices as soon as possible.

Related CVEs: CVE-2018-11457, CVE-2018-11458, CVE-2018-11459, CVE-2018-11460, CVE-2018-11461, CVE-2018-11462, CVE-2018-11463, CVE-2018-11464, CVE-2018-11465, CVE-2018-11466

Link 1

SSA-880233	**9.9**	Incorrect Session Validation Vulnerability in SINEMA Server	14/01/20 00:00	14/01/20 00:00	06/07/20 16:38

Access Type: Network

The latest update for SINEMA Server fixes a vulnerability that could allow authenticated users with a low-privileged account to perform firmware updates (as well as other administrative operations) on connected devices. Therefore, Siemens recommends to update the affected products.

Related CVEs: CVE-2019-10940

Link 1

SSA-110922	**9.8**	Web Vulnerability in TIM 1531 IRC	27/03/18 01:00	27/03/18 01:00	06/07/20 16:38

Access Type: Network

The latest update for TIM 1531 IRC fixes a security vulnerability that could allow unauthorized remote attackers to perform administrative operations on the device. Siemens recommends updating as soon as possible.

Related CVEs: CVE-2018-4841

Link 1

CVE-ID	SCORE (CVSS)	TITLE	PUBLISHED	MODIFIED	IDENTIFIED ON
SSA-189842	**9.8**	TCP URGENT/11 Vulnerabilities in RUGGEDCOM Win	10/09/19 01:00	10/09/19 01:00	06/07/20 16:38

Access Type: Network

RUGGEDCOM Win is affected by multiple security vulnerabilities. These vulnerabilities could allow an attacker to leverage various attacks, e.g. to execute arbitrary code over the network. The vulnerabilities affect the underlying Wind River VxWorks network stack and were recently patched by Wind River. Siemens is working on updates for the affected products, and recommends specific countermeasures until fixes are available.

Related CVEs: CVE-2019-12255, CVE-2019-12256, CVE-2019-12257, CVE-2019-12258, CVE-2019-12259, CVE-2019-12260, CVE-2019-12261, CVE-2019-12262, CVE-2019-12263, CVE-2019-12264, CVE-2019-12265

Link 1

CVE-ID	SCORE (CVSS)	TITLE	PUBLISHED	MODIFIED	IDENTIFIED ON
SSA-126840	**9.8**	Vulnerability in Communication Processor module CP 440-1 RNA	20/06/17 01:00	20/06/17 01:00	06/07/20 16:38

Access Type: Network

An unauthenticated remote user could perform administrative actions on the affected Communication Processor (CP) if network access (port 102/TCP) is available, and the CP's configuration is stored on the corresponding CPU.

Related CVEs: CVE-2017-6868

Link 1

CVE-ID	SCORE (CVSS)	TITLE	PUBLISHED	MODIFIED	IDENTIFIED ON
ICSA-19-211-01	**9.8**	(Urgent/11) Wind River VxWorks Vulnerabilities	30/07/19 01:00	31/07/19 01:00	06/07/20 16:38

CVE-ID	SCORE (CVSS)	TITLE	PUBLISHED	MODIFIED	IDENTIFIED ON

Access Type: Network

multiple vulnerabilities in Wind River’s VxWorks TCP/IP. Six of the 11 vulnerabilities have the potential to trigger remote code execution. Stack

Related CVEs: SSA-632562, BSECV-2019-05

Link 1

BASELINE DETAILS

Name	Transmission	Source	Destination	Communication Type	Access Type
S7Comm: Write var Area: Flags (M), ObtainByLID: 16	TCP / 102	10.10.10.30	10.10.10.10	Data Acquisition	Write
S7Comm: Write var Area: Flags (M), ObtainByLID: 18	TCP / 102	10.10.10.30	10.10.10.10	Data Acquisition	Write
S7Comm: Write var Area: Flags (M), ObtainByLID: 16	TCP / 102	10.10.10.20	10.10.10.10	Data Acquisition	Write
S7Comm: Write var Area: Flags (M), ObtainByLID: 17	TCP / 102	10.10.10.30	10.10.10.10	Data Acquisition	Write
S7Comm: Write var Area: Flags (M), ObtainByLID: 17	TCP / 102	192.168.1.10	10.10.10.10	Data Acquisition	Write
S7Comm: Write var Area: Flags (M), ObtainByLID: 16	TCP / 102	192.168.1.10	10.10.10.10	Data Acquisition	Write
S7Comm: Write var Area: Flags (M), ObtainByLID: 18	TCP / 102	192.168.1.10	10.10.10.10	Data Acquisition	Write
S7Comm: Read var Area: Flags (M), ObtainByLID: 16	TCP / 102	10.10.10.20	10.10.10.10	Data Acquisition	Read
S7Comm: Read var Area: Flags (M), ObtainByLID: 17	TCP / 102	10.10.10.20	10.10.10.10	Data Acquisition	Read
S7Comm: Read var Area: Flags (M), ObtainByLID: 18	TCP / 102	10.10.10.20	10.10.10.10	Data Acquisition	Read
S7Comm: Read var Area: Flags (M), ObtainByLID: 19	TCP / 102	10.10.10.20	10.10.10.10	Data Acquisition	Read
S7Comm: Read var Area: Flags (M), ObtainByLID: 20	TCP / 102	10.10.10.20	10.10.10.10	Data Acquisition	Read
S7Comm: Setup communication	TCP / 102	10.10.10.30	10.10.10.10	Protocol	None
S7Comm: Read var Area: Flags (M), ObtainByLID: 9	TCP / 102	10.10.10.30	10.10.10.10	Data Acquisition	Read
S7Comm: Read var	TCP / 102	10.10.10.30	10.10.10.10	Data Acquisition	Read

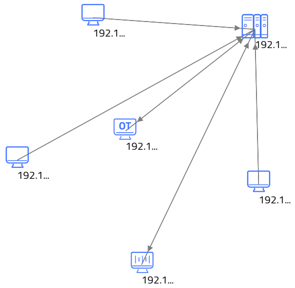
Area: Flags (M), ObtainByLID: 10					
S7Comm: Setup communication	TCP / 102	192.168.1.10	10.10.10.10	Protocol	None
S7Comm: Read var Area: Flags (M), ObtainByLID: 9	TCP / 102	192.168.1.10	10.10.10.10	Data Acquisition	Read
S7Comm: Read var Area: Flags (M), ObtainByLID: 10	TCP / 102	192.168.1.10	10.10.10.10	Data Acquisition	Read
ARP : Response for ipv4 address 10.10.10.20 with mac address 00:1c:06:27:64:11		00:1C:06:27:64:11	28:63:36:89:59:82	Network	None
ARP : Response for ipv4 address 10.10.10.30 with mac address 54:ee:75:3f:4a:db		54:EE:75:3F:4A:DB	28:63:36:89:59:82	Network	None

ASSET INFORMATION

Asset Name	Type	Site	Vendor
192.168.88.20	PLC	SolutionsPT	Phoenix Contact Electronics

IP	MAC	Protocols
192.168.88.20	00:A0:45:6F:4B:83	ARP, FTP, HTTP, ICMP, LDAPS, MODBUS, NETBIOS-NAME, POP3, PORTMAPPER, RDP, RLOGIN, RPC, SIP, SMTP, SSH, SSL, TACACS, TCP, TDS, TELNET, UDP, WHOIS

NETWORK COMMUNICATIONS



BASELINE DETAILS

Name	Transmission	Source	Destination	Communication Type	Access Type
RPC : Remote Call on Program: portmapper	TCP / 502	192.168.2.133	192.168.88.20	Operation	Execute
MODBUS: Read Device Identification (read code: Basic Device Identification, object ID: VendorName)	TCP / 502	192.168.2.133	192.168.88.20	Diagnosis	Read
MODBUS: Report Slave ID	TCP / 502	192.168.2.133	192.168.88.20	Diagnosis	Read
MODBUS: Read Device Identification (read code: Basic Device Identification, object ID: VendorName)	TCP / 502	192.168.2.44	192.168.88.20	Diagnosis	Read
MODBUS: Report Slave ID	TCP / 502	192.168.2.44	192.168.88.20	Diagnosis	Read
SIP: Request - OPTIONS	TCP / 502	192.168.2.133	192.168.88.20	Protocol	None
ARP : Request for ipv4 address 192.168.88.20		00:07:7C:1A:61:83	00:A0:45:6F:4B:83	Network	None
ARP : Response for ipv4 address 192.168.88.20 with mac address 00:a0:45:6f:4b:83		00:A0:45:6F:4B:83	00:07:7C:1A:61:83	Network	None
TCP from any port to port 2222	TCP / 2222	192.168.2.137	192.168.88.20	Other	None
TCP from any port to port 20000	TCP / 20000	192.168.2.137	192.168.88.20	Other	None
HTTP: OPTIONS for host 192.168.88.20, with no specified path	TCP / 80	192.168.2.137	192.168.88.20	Other	Read
HTTP: GET with no host or remote	TCP / 80	192.168.2.137	192.168.88.20	Other	Read

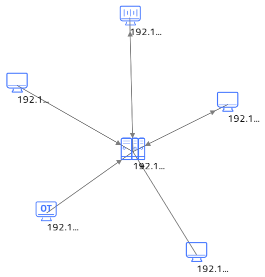
path information					
HTTP: GET for host: 192.168.88.20, remote path: *	TCP / 80	192.168.2.137	192.168.88.20	Other	Read
TCP from any port to port 102	TCP / 102	192.168.2.44	192.168.88.20	Other	None
ICMP: Echo (ping) requestcode 0		192.168.2.44	192.168.88.20	Network	None
ICMP: Echo (ping) replycode 0		192.168.88.20	192.168.2.44	Network	None
ICMP: Type 155code 198		192.168.2.44	192.168.88.20	Network	None
ICMP: Type 219code 156		192.168.2.44	192.168.88.20	Network	None
ICMP: Type 113code 13		192.168.2.44	192.168.88.20	Network	None
ICMP: Type 28code 193		192.168.2.44	192.168.88.20	Network	None
ICMP: Type 155code 139		192.168.2.44	192.168.88.20	Network	None

ASSET INFORMATION

Asset Name	Type	Site	Vendor
192.168.88.50	PLC	SolutionsPT	Red Lion Controls

IP	MAC	Protocols
192.168.88.50	00:05:E4:01:24:D3	ARP, FTP, HTTP, ICMP, LDAPS, MODBUS, NETBIOS-NAME, POP3, PORTMAPPER, RDP, RLOGIN, RPC, SIP, SMTP, SSH, SSL, TACACS, TCP, TDS, TELNET, UDP, WHOIS

NETWORK COMMUNICATIONS



BASELINE DETAILS

Name	Transmission	Source	Destination	Communication Type	Access Type
RPC : Remote Call on Program: portmapper	TCP / 502	192.168.2.133	192.168.88.50	Operation	Execute
RPC : Remote Call on Program: portmapper	TCP / 502	192.168.2.166	192.168.88.50	Operation	Execute
MODBUS: Read Coils (from: 0, count: 65535)	TCP / 502	192.168.2.166	192.168.88.50	Data Acquisition	Read
MODBUS: Read Coils	TCP / 502	192.168.2.166	192.168.88.50	Data Acquisition	Read
MODBUS: Read Device Identification (read code: Basic Device Identification, object ID: VendorName)	TCP / 502	192.168.2.133	192.168.88.50	Diagnosis	Read
MODBUS: Report Slave ID	TCP / 502	192.168.2.133	192.168.88.50	Diagnosis	Read
MODBUS: Read Input Registers (from: 0, count: 1)	TCP / 502	192.168.2.166	192.168.88.50	Data Acquisition	Read
MODBUS: Read Holding Registers (from: 0, count: 1)	TCP / 502	192.168.2.166	192.168.88.50	Data Acquisition	Read
MODBUS: Read Discrete Inputs (from: 0, count: 1)	TCP / 502	192.168.2.166	192.168.88.50	Data Acquisition	Read
MODBUS: Read Device Identification (read code: Regular Device Identification, object ID: VendorName)	TCP / 502	192.168.2.166	192.168.88.50	Diagnosis	Read
MODBUS: Read Device Identification (read code: Basic Device Identification,	TCP / 502	192.168.2.44	192.168.88.50	Diagnosis	Read

object ID: VendorName)					
MODBUS: Report Slave ID	TCP / 502	192.168.2.44	192.168.88.50	Diagnosis	Read
SIP: Request - OPTIONS	TCP / 502	192.168.2.166	192.168.88.50	Protocol	None
TCP from any port to port 3306	TCP / 3306	192.168.2.137	192.168.88.50	Other	None
TCP from any port to port 1723	TCP / 1723	192.168.2.137	192.168.88.50	Other	None
TCP from any port to port 1025	TCP / 1025	192.168.2.137	192.168.88.50	Other	None
TCP from any port to port 587	TCP / 587	192.168.2.137	192.168.88.50	Other	None
ARP : Response for ipv4 address 192.168.88.50 with mac address 00:05:e4:01:24:d3		00:05:E4:01:24:D3	00:07:7C:1A:61:83	Network	None
TCP from any port to port 2222	TCP / 2222	192.168.2.137	192.168.88.50	Other	None
TCP from any port to port 20000	TCP / 20000	192.168.2.137	192.168.88.50	Other	None
ARP : Request for ipv4 address 192.168.88.50		00:07:7C:1A:61:83	00:05:E4:01:24:D3	Network	None

ASSET INFORMATION

Asset Name	Type	Site	Vendor
10.10.10.20	HMI	SolutionsPT	Siemens

IP	MAC	Protocols
10.10.10.20	00:1C:06:27:64:11	ARP, S7COMM

NETWORK COMMUNICATIONS

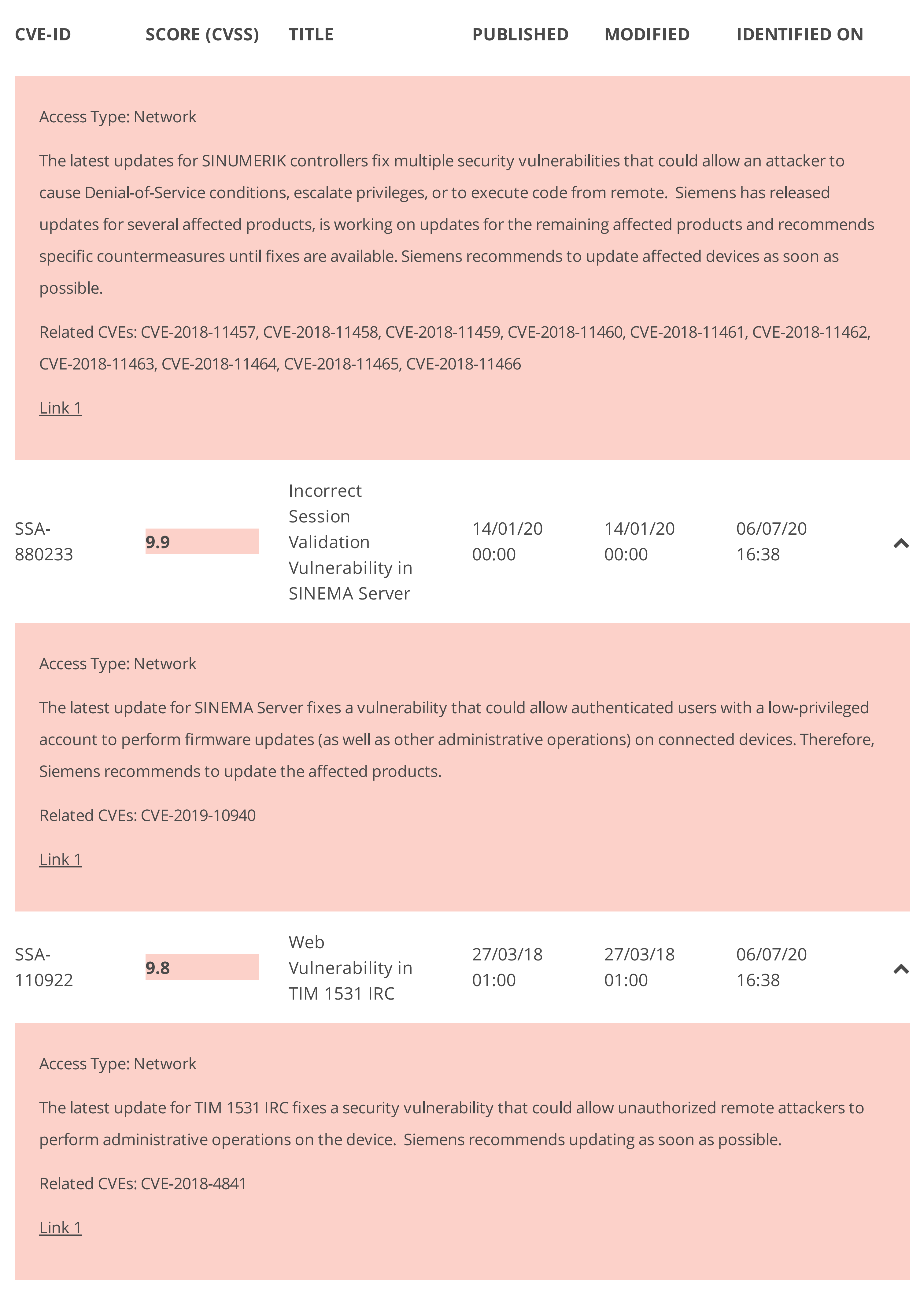
VENDOR MATCH CVES

This table lists assets that run vulnerable software versions and can be leveraged by attackers for various malicious purposes such as, remote code execution, DDOS, etc.

Vulnerabilities are matched against these assets' vendor name

<table>
<tr><th>CVE-ID</th><th>SCORE (CVSS)</th><th>TITLE</th><th>PUBLISHED</th><th>MODIFIED</th><th>IDENTIFIED ON</th></tr>
<tr><td>SSA-902727</td><td>10.0</td><td>Multiple Vulnerabilities in Licensing Software for SISHIP Automation</td><td>14/05/19 01:00</td><td>14/05/19 01:00</td><td>06/07/20 16:38</td></tr>
<tr><td colspan="6">Access Type: Network
Multiple vulnerabilities have been identified in the WibuKey Digital Rights Management (DRM) solution, which affect SISHIP Automation Solutions. Siemens recommends users to apply the updates to WibuKey Digital Rights Management (DRM) provided by WIBU SYSTEMS AG.
Related CVEs: CVE-2018-3989, CVE-2018-3990, CVE-2018-3991
Link 1</td></tr>
<tr><td>CVE-2016-7112</td><td>10.0</td><td>Authentication Bypass Vulnerability in SIPROTEC</td><td>09/05/16 01:00</td><td>22/03/18 00:00</td><td>06/07/20 16:38</td></tr>
<tr><td colspan="6">Access Type: Network
Attackers with network access to the device’s web interface (Port 80/TCP) could circumvent authentication and perform certain administrative operations.
Related CVEs: SSA-630413 , ICSA-17-187-03
Link 1</td></tr>
<tr><td>ICSA-16-040-02</td><td>10.0</td><td>Denial-of-service condition or a replay attack</td><td>22/03/16 00:00</td><td>22/03/16 00:00</td><td>06/07/20 16:38</td></tr>
</table>

<table>
<tr><th>CVE-ID</th><th>SCORE (CVSS)</th><th>TITLE</th><th>PUBLISHED</th><th>MODIFIED</th><th>IDENTIFIED ON</th></tr>
<tr><td colspan="6">Access Type: Unknown
Successful exploitation of these vulnerabilities could result in a denial-of-service condition or a replay attack on the affected devices
Related CVEs:
Link 1</td></tr>
<tr><td>SSA-982399</td><td>**10.0**</td><td>Missing Authentication in TIM 1531 IRC Modules</td><td>11/12/18 00:00</td><td>17/12/18 00:00</td><td>06/07/20 16:38</td></tr>
<tr><td colspan="6">Access Type: Network
The latest update for TIM 1531 IRC fixes a vulnerability. The devices was missing proper authentication when connecting on port 102/tcp, although configured. An attacker needs to be able to connect to port 102/tcp of an affected device in order to exploit this vulnerability. The vulnerability could allow an attacker to perform administrative operations. Siemens has released updates for TIM 1531 IRC modules.
Related CVEs: CVE-2018-13816
Link 1</td></tr>
<tr><td>SSA-170881</td><td>**10.0**</td><td>Vulnerabilities in SINUMERIK Controllers</td><td>11/12/18 00:00</td><td>12/03/19 00:00</td><td>06/07/20 16:38</td></tr>
</table>



<table>
<tr><th>CVE-ID</th><th>SCORE (CVSS)</th><th>TITLE</th><th>PUBLISHED</th><th>MODIFIED</th><th>IDENTIFIED ON</th></tr>
<tr><td colspan="6">Access Type: Network
The latest updates for SINUMERIK controllers fix multiple security vulnerabilities that could allow an attacker to cause Denial-of-Service conditions, escalate privileges, or to execute code from remote. Siemens has released updates for several affected products, is working on updates for the remaining affected products and recommends specific countermeasures until fixes are available. Siemens recommends to update affected devices as soon as possible.
Related CVEs: CVE-2018-11457, CVE-2018-11458, CVE-2018-11459, CVE-2018-11460, CVE-2018-11461, CVE-2018-11462, CVE-2018-11463, CVE-2018-11464, CVE-2018-11465, CVE-2018-11466
Link 1</td></tr>
<tr><td>SSA-880233</td><td><b>9.9</b></td><td>Incorrect Session Validation Vulnerability in SINEMA Server</td><td>14/01/20 00:00</td><td>14/01/20 00:00</td><td>06/07/20 16:38</td></tr>
<tr><td colspan="6">Access Type: Network
The latest update for SINEMA Server fixes a vulnerability that could allow authenticated users with a low-privileged account to perform firmware updates (as well as other administrative operations) on connected devices. Therefore, Siemens recommends to update the affected products.
Related CVEs: CVE-2019-10940
Link 1</td></tr>
<tr><td>SSA-110922</td><td><b>9.8</b></td><td>Web Vulnerability in TIM 1531 IRC</td><td>27/03/18 01:00</td><td>27/03/18 01:00</td><td>06/07/20 16:38</td></tr>
<tr><td colspan="6">Access Type: Network
The latest update for TIM 1531 IRC fixes a security vulnerability that could allow unauthorized remote attackers to perform administrative operations on the device. Siemens recommends updating as soon as possible.
Related CVEs: CVE-2018-4841
Link 1</td></tr>
</table>

<table>
<tr><th>CVE-ID</th><th>SCORE (CVSS)</th><th>TITLE</th><th>PUBLISHED</th><th>MODIFIED</th><th>IDENTIFIED ON</th><th></th></tr>
<tr><td>SSA-189842</td><td><b>9.8</b></td><td>TCP URGENT/11 Vulnerabilities in RUGGEDCOM Win</td><td>10/09/19 01:00</td><td>10/09/19 01:00</td><td>06/07/20 16:38</td><td>⌃</td></tr>
<tr><td colspan="7">Access Type: Network
RUGGEDCOM Win is affected by multiple security vulnerabilities. These vulnerabilities could allow an attacker to leverage various attacks, e.g. to execute arbitrary code over the network. The vulnerabilities affect the underlying Wind River VxWorks network stack and were recently patched by Wind River. Siemens is working on updates for the affected products, and recommends specific countermeasures until fixes are available.
Related CVEs: CVE-2019-12255, CVE-2019-12256, CVE-2019-12257, CVE-2019-12258, CVE-2019-12259, CVE-2019-12260, CVE-2019-12261, CVE-2019-12262, CVE-2019-12263, CVE-2019-12264, CVE-2019-12265
Link 1</td></tr>
<tr><td>SSA-126840</td><td><b>9.8</b></td><td>Vulnerability in Communication Processor module CP 440-1 RNA</td><td>20/06/17 01:00</td><td>20/06/17 01:00</td><td>06/07/20 16:38</td><td>⌃</td></tr>
<tr><td colspan="7">Access Type: Network
An unauthenticated remote user could perform administrative actions on the affected Communication Processor (CP) if network access (port 102/TCP) is available, and the CP's configuration is stored on the corresponding CPU.
Related CVEs: CVE-2017-6868
Link 1</td></tr>
<tr><td>ICSA-19-211-01</td><td><b>9.8</b></td><td>(Urgent/11) Wind River VxWorks Vulnerabilities</td><td>30/07/19 01:00</td><td>31/07/19 01:00</td><td>06/07/20 16:38</td><td>⌃</td></tr>
</table>

CVE-ID	SCORE (CVSS)	TITLE	PUBLISHED	MODIFIED	IDENTIFIED ON
Access Type: Network multiple vulnerabilities in Wind River’s VxWorks TCP/IP. Six of the 11 vulnerabilities have the potential to trigger remote code execution. Stack Related CVEs: SSA-632562, BSECV-2019-05 Link 1					

BASELINE DETAILS

Name	Transmission	Source	Destination	Communication Type	Access Type
S7Comm: Write var Area: Flags (M), ObtainByLID: 16	TCP / 102	10.10.10.20	10.10.10.10	Data Acquisition	Write
S7Comm: Read var Area: Flags (M), ObtainByLID: 16	TCP / 102	10.10.10.20	10.10.10.10	Data Acquisition	Read
S7Comm: Read var Area: Flags (M), ObtainByLID: 17	TCP / 102	10.10.10.20	10.10.10.10	Data Acquisition	Read
S7Comm: Read var Area: Flags (M), ObtainByLID: 18	TCP / 102	10.10.10.20	10.10.10.10	Data Acquisition	Read
S7Comm: Read var Area: Flags (M), ObtainByLID: 19	TCP / 102	10.10.10.20	10.10.10.10	Data Acquisition	Read
S7Comm: Read var Area: Flags (M), ObtainByLID: 20	TCP / 102	10.10.10.20	10.10.10.10	Data Acquisition	Read
ARP : Response for ipv4 address 10.10.10.20 with mac address 00:1c:06:27:64:11		00:1C:06:27:64:11	28:63:36:89:59:82	Network	None
ARP : Response for ipv4 address 10.10.10.10 with mac address 28:63:36:89:59:82		28:63:36:89:59:82	00:1C:06:27:64:11	Network	None

ASSET INFORMATION

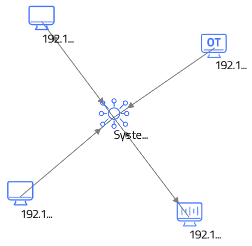
Asset Name	Type	Site	Vendor
System Name	Networking	SolutionsPT	Siemens

Model	Firmware	IP	MAC
RS910-48-D-S1-TX01-MC	v3.8.0	192.168.88.95	00:0A:DC:5B:27:A0

Protocols

ARP, DNP3, FTP, HTTP, ICMP, LDAPS, MODBUS, NETBIOS-NAME, POP3, PORTMAPPER, RDP, RLOGIN, RPC, SIP, SMTP, SSH, SSL, TACACS, TCP, TDS, TELNET, UDP, WHOIS

NETWORK COMMUNICATIONS



BASELINE DETAILS

Name	Transmission	Source	Destination	Communication Type	Access Type
RPC : Remote Call on Program: portmapper	TCP / 502	192.168.2.133	192.168.88.95	Operation	Execute
RPC : Remote Call on Program: portmapper	TCP / 502	192.168.2.166	192.168.88.95	Operation	Execute
DNP3: Request link status	TCP / 20000	192.168.2.166	192.168.88.95	Protocol	None
MODBUS: Read Device Identification (read code: Basic Device Identification, object ID: VendorName)	TCP / 502	192.168.2.133	192.168.88.95	Diagnosis	Read
MODBUS: Report Slave ID	TCP / 502	192.168.2.133	192.168.88.95	Diagnosis	Read
MODBUS: Read Device Identification (read code: Regular Device Identification, object ID: VendorName)	TCP / 502	192.168.2.166	192.168.88.95	Diagnosis	Read
TELNET: data sent	TCP / 23	192.168.2.137	192.168.88.95	Remote Connection	None
SSH : Connection request. Client uses protocol version 1.5	TCP / 22	192.168.2.137	192.168.88.95	Remote Connection	None
SSH : Connection request. Client uses protocol version 2.0	TCP / 22	192.168.2.137	192.168.88.95	Remote Connection	None
SIP: Request - OPTIONS	TCP / 502	192.168.2.133	192.168.88.95	Protocol	None
SSH : Connection request. Client uses protocol version 1.5	TCP / 22	192.168.2.166	192.168.88.95	Remote Connection	None
SSH : Connection	TCP / 22	192.168.2.166	192.168.88.95	Remote	None

request. Client uses protocol version 2.0				Connection	
TELNET: data sent	TCP / 23	192.168.2.166	192.168.88.95	Remote Connection	None
SIP: Request - OPTIONS	TCP / 502	192.168.2.166	192.168.88.95	Protocol	None
TCP from any port to port 2222	TCP / 2222	192.168.2.137	192.168.88.95	Other	None
TCP from any port to port 20000	TCP / 20000	192.168.2.137	192.168.88.95	Other	None
ARP : Request for ipv4 address 192.168.88.95		00:07:7C:1A:61:83	00:0A:DC:5B:27:A0	Network	None
ARP : Response for ipv4 address 192.168.88.95 with mac address 00:0a:dc:5b:27:a0		00:0A:DC:5B:27:A0	00:07:7C:1A:61:83	Network	None
TCP from any port to port 144	TCP / 144	192.168.2.137	192.168.88.95	Other	None
TCP from any port to port 2005	TCP / 2005	192.168.2.137	192.168.88.95	Other	None
TCP from any port to port 648	TCP / 648	192.168.2.137	192.168.88.95	Other	None
TCP from any port to port 30951	TCP / 30951	192.168.2.137	192.168.88.95	Other	None
TCP from any port to port 50800	TCP / 50800	192.168.2.137	192.168.88.95	Other	None
TCP from any port to port 5902	TCP / 5902	192.168.2.137	192.168.88.95	Other	None
TCP from any port to port 544	TCP / 544	192.168.2.137	192.168.88.95	Other	None
TCP from any port to port 500	TCP / 500	192.168.2.137	192.168.88.95	Other	None
TCP from any port to port 1042	TCP / 1042	192.168.2.137	192.168.88.95	Other	None
TCP from any port to port 4343	TCP / 4343	192.168.2.137	192.168.88.95	Other	None