



**41**  
Vulnerable  
Devices



**26**  
Devices Needing  
Improvement



**124**  
Secure Devices



- Q All devices are authorized
- Q 29 Internet connections detected
- Q 33 connections to ICS networks detected
- Q Firewall rules: 0 out of 0 firewall rules are vulnerable
- Q No backup servers detected
- Q 7 Devices accessible remotely
- Q No engineering stations detected
- Q 1 Scanning device detected
- Q No AV software detected
- Q 3 top attack vectors generated (highest risk)



## Table of Contents

---

Executive Summary .....	3
Overview .....	5
Terms .....	6
Top Vulnerable Devices .....	7
Network Security Risks .....	14
Industrial Malware Indicators .....	14
Weak Firewall Rules .....	14
Unauthorized Devices .....	14
Internet Connections .....	14
Illegal Traffic by Firewall Rules .....	14
Access Points .....	14
Connections to ICS networks .....	14
Network Operations .....	18
Protocol Problems .....	18
Protocol Data Volumes .....	18
Disconnections .....	18
Backup server .....	18
IP Networks .....	18
Attack Vector #1 .....	22
Attack Vector #2 .....	23
Attack Vector #3 .....	24
Mitigation .....	25

## Executive Summary

### Device Security

Vendor	Quantity	Security Score Range
VMWARE INC.	20	35% - 100%
ROCKWELL AUTOMATION	19	32% - 100%
HEWLETT PACKARD	16	35% - 100%
DELL INC.	8	16% - 100%
UNIVERSAL GLOBAL SCIENTIFIC INDUSTRIAL CO. LTD.	6	35% - 100%
FREEWAVE TECHNOLOGIES	5	100%
INTEL CORPORATE	5	35% - 80%
SIEMENS AG	5	32% - 100%
YOKOGAWA DIGITAL COMPUTER CORPORATION	5	100%
ABB OY DRIVES	4	100%
FISHER CONTROLS	4	100%
FISHER-ROSEMOUNT SYSTEMS INC.	3	100%
TELEMECANIQUE ELECTRIQUE	3	80% - 100%
COMPAL INFORMATION (KUNSHAN) CO. LTD.	2	40% - 100%
D-LINK CORPORATION	2	80% - 89%
HONEYWELL INTERNATIONAL HPS	2	60% - 70%
MICRO-STAR INT'L CO. LTD.	2	70% - 100%
PALO ALTO NETWORKS	2	40% - 99%
PCS SYSTEMTECHNIK GMBH	2	40% - 100%
PRO-VISION INC.	2	100%
ABB INDUSTRIAL SYSTEMS AB	1	69%
APPLE INC.	1	40%
ARUBA A HEWLETT PACKARD ENTERPRISE COMPANY	1	100%
CANON INC.	1	100%
CISCO SYSTEMS INC	1	100%
GIGA-BYTE TECHNOLOGY CO.LTD.	1	100%
HON HAI PRECISION IND. CO.LTD.	1	100%
INTEL CORPORATION	1	80%
INTELLIGENT PLATFORMS LLC.	1	80%
INVENTEC CORPORATION	1	100%
LCFC(HEFEI) ELECTRONICS TECHNOLOGY CO. LTD.	1	35%
MICROSOFT CORPORATION	1	35%

Vendor	Quantity	Security Score Range
NETGEAR	1	70%
RASPBERRY PI FOUNDATION	1	80%
RUGGEDCOM INC.	1	32%
SQUARE D COMPANY	1	100%
TP-LINK TECHNOLOGIES CO.LTD.	1	100%
VIVAVIS AG	1	59%
WISTRON CORPORATION	1	80%

## Attack Vectors

No.	Entry Point	Target	Score
#1	192.168.90.109	192.168.10.3	93
#2	192.168.90.109	192.168.90.7	88
#3	192.168.90.109	192.168.90.118	88

## Network Security Risks

Category	Results
Internet Connections	29
Connections to ICS networks	21
Access Points	15
Industrial Malware Indicators	11
Wireless Access Points	2

## Network Operations

Category	Results
Protocol Problems	41
Disconnections	2

## Mitigation

Category	Maximum Security Impact
Check any Internet Connections ensuring all are allowed. Consider removing unnecessary connections or using an offline-proxy or a Unidirectional Security Gateway	14%
Upgrade firmware to the latest version (Devices: 6)	12%
Install an Antivirus solution to increase protection of the workstations	10%
Investigate all malware indicators (Contact your incident response team or support.microsoft.com). When assured the problem is solved, acknowledge the alert	7%
Install a backup server in the network	5%
Investigate and acknowledge all unacknowledge alerts	4%

## Overview

---

The Risk Assessment report is a comprehensive security vulnerability assessment report that is generated by Azure Defender for IoT, based on network analysis using deep packet inspection, several behavioral modeling engines, and a SCADA-specific state machine design.

It is recommended to upload additional information about the devices (such as authorized devices, firmware and patch versions of a device) using the Import Settings tab to enhance and improve the accuracy of the analysis.

The report generates a security score for each network device, as well as an overall network security score. This score is based on a calculation that aggregates device security scores, related vulnerabilities, configuration issues and other network risks. The report provides mitigation recommendations that will help you improve your current security score.

## Terms

---

**Attack Vector** - A chain of devices that can be used by an attacker to compromise a target. The first of these, is a device that is likely to be accessible to the attacker (e.g Internet connection). Each device in the chain is connected to the adjacent device and the attacker will use this connection to get access to each subsequent device. The chain ends with an important device which is the target of the attack. A file can be imported with additional device information such as the most valuable/important devices, firmware and patch versions of a device, and more.

**CVE** - Common Vulnerabilities and Exposures, is a standard system that provides a reference method for publicly known information security vulnerabilities and exposures.

**CVSS** - Common Vulnerability Scoring System, is a free and open industry standard for assessing the severity of computer system security vulnerabilities.

**Device Patches** - Hotfixes or firmware upgrades installed on a device to protect from a CVE threat.

**Devices Needing Improvement** - Devices with a security score between 70% and 89%.

**Devices Security Score** - A score between 0% and 100% that reflects the device's security, where 100% is mostly secure. The Device Security Score is created using the CVSS score of all the device's CVE and other vulnerabilities, configuration issues such as open ports, internet connections and loose firewall rules.

**Programming Devices** - Workstations or servers used by an engineer to configure or program SCADA devices.

**Firewall Rules** - Firewall rules exported from various firewall products, loaded into the sensor (See page "Import Settings").

**Important Devices** - Devices that were marked as valuable by the user. The Risk Assessment Score gives a higher weighting to the security scores of "Important Devices", as these devices are used as the targets of attack vectors.

**Known Scanner** - A device that periodically scans the network or communicates with many other devices.

**Secure Devices** - Devices with a security score above 90%.

**Security Score** - A total score between 0% and 100% that reflects the device's security, where 100% is mostly secure. The Security Score is based on a calculation that aggregates all device's security scores along with more vulnerabilities and configuration issues.

**Vulnerable Devices** - Devices with a security score below 70%.

## Top Vulnerable Devices listed by lowest security score

10.10.10.25

10.10.10.25

Windows XP

Security Score 16%

★ 1 Unacknowledged Alert exists

Most Severe CVE

This device is running on Windows XP, which is not supported anymore and has no security updates since April 2014.

HOBARTRANCH764

10.150.90.129

Windows 7

Security Score 16%

★ 1 Unacknowledged Alert exists

Most Severe CVE

CVE ID	Score	Description
CVE-2014-1776	10.0	Use-after-free vulnerability in Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via vectors related to the CMarkup::IsConnectedToPrimaryMarkup function, as exploited in the wild in April 2014. NOTE: this issue originally emphasized VGX.DLL, but Microsoft clarified that "VGX.DLL does not contain the vulnerable code leveraged in this exploit. Disabling VGX.DLL is an exploit-specific workaround that provides an immediate, effective workaround to help block known attacks."
CVE-2014-1763	10.0	Use-after-free vulnerability in Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code and bypass a sandbox protection mechanism via unspecified vectors, as demonstrated by VUPEN during a Pwn2Own competition at CanSecWest 2014.
CVE-2014-1764	10.0	Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code and bypass a sandbox protection mechanism by leveraging "object confusion" in a broker process, as demonstrated by VUPEN during a Pwn2Own competition at CanSecWest 2014.
CVE-2010-2550	10.0	The SMB Server in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly validate fields in an SMB request, which allows remote attackers to execute arbitrary code via a crafted SMB packet, aka "SMB Pool Overflow Vulnerability."
CVE-2011-1868	10.0	The Distributed File System (DFS) implementation in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 does not properly validate fields in DFS responses, which allows remote DFS servers to execute arbitrary code via a crafted response, aka "DFS Memory Corruption Vulnerability."



**USER-PC**  
192.168.1.1

Windows Server 2016

Security Score 28%



## ★ 2 Unacknowledged Alerts exist

### Most Severe CVE

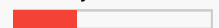
CVE ID	Score	Description
CVE-2020-0609	10.0	A remote code execution vulnerability exists in Windows Remote Desktop Gateway (RD Gateway) when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Gateway (RD Gateway) Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0610.
CVE-2020-0610	10.0	A remote code execution vulnerability exists in Windows Remote Desktop Gateway (RD Gateway) when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Gateway (RD Gateway) Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0609.
CVE-2020-1350	10.0	A remote code execution vulnerability exists in Windows Domain Name System servers when they fail to properly handle requests, aka 'Windows DNS Server Remote Code Execution Vulnerability'.
CVE-2020-17051	10.0	Windows Network File System Remote Code Execution Vulnerability
CVE-2020-0690	10.0	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'.



**192.168.10.3**  
192.168.10.3

SIEMENS AG

Security Score 32%



## ★ Marked As Important

## ★ 1 Unacknowledged Alert exists

### Ports In Use

- TCP PORT 102 (ISO Transport)



## Most Severe CVE

CVE ID	Score	Description
CVE-2015-2177	7.8	Siemens SIMATIC S7-300 CPU devices allow remote attackers to cause a denial of service (defect-mode transition) via crafted packets on (1) TCP port 102 or (2) Profibus.
CVE-2018-16561	7.8	A vulnerability has been identified in SIMATIC S7-300 CPUs (All versions < V3.X.16). The affected CPUs improperly validate S7 communication packets which could cause a Denial-of-Service condition of the CPU. The CPU will remain in DEFECT mode until manual restart. Successful exploitation requires an attacker to be able to send a specially crafted S7 communication packet to a communication interface of the CPU. This includes Ethernet, PROFIBUS, and Multi Point Interfaces (MPI). No user interaction or privileges are required to exploit the security vulnerability. The vulnerability could allow causing a Denial-of-Service condition of the core functionality of the CPU, compromising the availability of the system. At the time of advisory publication no public exploitation of this security vulnerability was known. Siemens confirms the security vulnerability and provides mitigations to resolve the security issue.
CVE-2019-18336	7.8	A vulnerability has been identified in SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V3.X.17), SIMATIC TDC CP51M1 (All versions < V1.1.8), SIMATIC TDC CPU555 (All versions < V1.1.1), SINUMERIK 840D sl (All versions < V4.8.6), SINUMERIK 840D sl (All versions < V4.94). Specially crafted packets sent to port 102/tcp (Profinet) could cause the affected device to go into defect mode. A restart is required in order to recover the system. Successful exploitation requires an attacker to have network access to port 102/tcp, with no authentication. No user interaction is required. At the time of advisory publication no public exploitation of this security vulnerability was known.
CVE-2016-9158	7.8	A vulnerability has been identified in SIMATIC S7-300 CPU family (All versions), SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V6 and below CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 V6 and earlier CPU family (All versions), SIMATIC S7-400 V7 CPU family (All versions). Specially crafted packets sent to port 80/tcp could cause the affected devices to go into defect mode. A cold restart is required to recover the system.
CVE-2017-12741	7.8	A vulnerability has been identified in Development/Evaluation Kits for PROFINET IO: DK Standard Ethernet Controller, Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200, Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200P, SIMATIC Compact Field Unit, SIMATIC ET200AL, SIMATIC ET200M (incl. SIPLUS variants), SIMATIC ET200MP IM155-5 PN BA (incl. SIPLUS variants), SIMATIC ET200MP IM155-5 PN HF (incl. SIPLUS variants), SIMATIC ET200MP IM155-5 PN ST (incl. SIPLUS variants), SIMATIC ET200S (incl. SIPLUS variants), SIMATIC ET200SP IM155-6 PN BA (incl. SIPLUS variants), SIMATIC ET200SP IM155-6 PN HA (incl. SIPLUS variants), SIMATIC ET200SP IM155-6 PN HF (incl. SIPLUS variants), SIMATIC ET200SP IM155-6 PN HS (incl. SIPLUS variants), SIMATIC ET200SP IM155-6 PN ST (incl. SIPLUS variants), SIMATIC ET200ecoPN (except 6ES7141-6BG00-0BB0, 6ES7141-6BH00-0BB0, 6ES7142-6BG00-0BB0, 6ES7142-6BR00-0BB0, 6ES7143-6BH00-0BB0, 6ES7146-6FF00-0AB0, 6ES7148-6JD00-0AB0 and 6ES7148-6JG00-0BB0), SIMATIC ET200pro, SIMATIC PN/PN Coupler (incl. SIPLUS NET variants), SIMATIC S7-1200 CPU family (incl. SIPLUS variants), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants), SIMATIC S7-1500 Software Controller, SIMATIC S7-200 Smart, SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants), SIMATIC S7-400 H V6 CPU family and below (incl. SIPLUS variants), SIMATIC S7-400 PN/DP V6 CPU family and below (incl. SIPLUS variants), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants), SIMATIC S7-410 V8 CPU family (incl. SIPLUS variants), SIMATIC TDC CP51M1, SIMATIC TDC CPU555, SIMATIC WinAC RTX (F) 2010, SIMOCODE pro V EIP (incl. SIPLUS variants), SIMOCODE pro V PN (incl. SIPLUS variants), SIMOTION C, SIMOTION D (incl. SIPLUS variants), SIMOTION D4xx V4.4 for SINAMICS SM150i-2 w. PROFINET (incl. SIPLUS variants), SIMOTION P V4.4 and V4.5, SIMOTION P V5, SINAMICS DCM w. PN, SINAMICS DCP w. PN, SINAMICS G110M w. PN, SINAMICS G120(C/P/D) w. PN (incl. SIPLUS variants), SINAMICS G130 V4.7 w. PN, SINAMICS G130 V4.8 w. PN, SINAMICS G150 V4.7 w. PN, SINAMICS G150 V4.8 w. PN, SINAMICS G150 V4.7 w. PROFINET, SINAMICS GM150 V4.7 w. PROFINET, SINAMICS S110 w. PN, SINAMICS S120 V4.7 SP1 w. PN (incl. SIPLUS variants), SINAMICS S120 V4.7 w. PN (incl. SIPLUS variants), SINAMICS S120 V4.8 w. PN (incl. SIPLUS variants), SINAMICS S120 prior to V4.7 w. PN (incl. SIPLUS variants), SINAMICS S150 V4.7 w. PN, SINAMICS S150 V4.8 w. PN, SINAMICS SL150 V4.7.0 w. PROFINET, SINAMICS SL150 V4.7.4 w. PROFINET, SINAMICS SL150 V4.7.5 w. PROFINET, SINAMICS SM120 V4.7 w. PROFINET, SINAMICS V90 w. PN, SINUMERIK 840D sl, SIRIUS Soft Starter 3RW44 PN. Specially crafted packets sent to port 161/udp could cause a Denial-of-Service condition. The affected devices must be restarted manually.



192.168.110.6  
192.168.110.6

ROCKWELL AUTOMATION

Security Score 32%


## ★ 1 Unacknowledged Alert exists

### Ports In Use

- TCP PORT 44818 (Ethernet/IP)

### Most Severe CVE

CVE ID	Score	Description
CVE-2012-6437	10.0	Rockwell Automation EtherNet/IP products; 1756-ENBT, 1756-EWEB, 1768-ENBT, and 1768-EWEB communication modules; CompactLogix L32E and L35E controllers; 1788-ENBT FLEXLogix adapter; 1794-AENTR FLEX I/O EtherNet/IP adapter; ControlLogix 18 and earlier; CompactLogix 18 and earlier; GuardLogix 18 and earlier; SoftLogix 18 and earlier; CompactLogix controllers 19 and earlier; SoftLogix controllers 19 and earlier; ControlLogix controllers 20 and earlier; GuardLogix controllers 20 and earlier; and MicroLogix 1100 and 1400 do not properly perform authentication for Ethernet firmware updates, which allows remote attackers to execute arbitrary code via a Trojan horse update image.
CVE-2012-6440	9.3	The web-server password-authentication functionality in Rockwell Automation EtherNet/IP products; 1756-ENBT, 1756-EWEB, 1768-ENBT, and 1768-EWEB communication modules; CompactLogix L32E and L35E controllers; 1788-ENBT FLEXLogix adapter; 1794-AENTR FLEX I/O EtherNet/IP adapter; ControlLogix 18 and earlier; CompactLogix 18 and earlier; GuardLogix 18 and earlier; SoftLogix 18 and earlier; CompactLogix controllers 19 and earlier; ControlLogix controllers 20 and earlier; GuardLogix controllers 20 and earlier; and MicroLogix 1100 and 1400 allows man-in-the-middle attackers to conduct replay attacks via HTTP traffic.
CVE-2012-6439	8.5	Rockwell Automation EtherNet/IP products; 1756-ENBT, 1756-EWEB, 1768-ENBT, and 1768-EWEB communication modules; CompactLogix L32E and L35E controllers; 1788-ENBT FLEXLogix adapter; 1794-AENTR FLEX I/O EtherNet/IP adapter; ControlLogix 18 and earlier; CompactLogix 18 and earlier; GuardLogix 18 and earlier; SoftLogix 18 and earlier; CompactLogix controllers 19 and earlier; SoftLogix controllers 19 and earlier; ControlLogix controllers 20 and earlier; GuardLogix controllers 20 and earlier; and MicroLogix 1100 and 1400 allow remote attackers to cause a denial of service (control and communication outage) via a CIP message that modifies the (1) configuration or (2) network parameters.
CVE-2012-6435	7.8	Rockwell Automation EtherNet/IP products; 1756-ENBT, 1756-EWEB, 1768-ENBT, and 1768-EWEB communication modules; CompactLogix L32E and L35E controllers; 1788-ENBT FLEXLogix adapter; 1794-AENTR FLEX I/O EtherNet/IP adapter; ControlLogix 18 and earlier; CompactLogix 18 and earlier; GuardLogix 18 and earlier; SoftLogix 18 and earlier; CompactLogix controllers 19 and earlier; SoftLogix controllers 19 and earlier; ControlLogix controllers 20 and earlier; GuardLogix controllers 20 and earlier; and MicroLogix 1100 and 1400 allow remote attackers to cause a denial of service (control and communication outage) via a CIP message that specifies a logic-execution stop and fault.
CVE-2012-6436	7.8	Buffer overflow in Rockwell Automation EtherNet/IP products; 1756-ENBT, 1756-EWEB, 1768-ENBT, and 1768-EWEB communication modules; CompactLogix L32E and L35E controllers; 1788-ENBT FLEXLogix adapter; 1794-AENTR FLEX I/O EtherNet/IP adapter; ControlLogix 18 and earlier; CompactLogix 18 and earlier; GuardLogix 18 and earlier; SoftLogix 18 and earlier; CompactLogix controllers 19 and earlier; SoftLogix controllers 19 and earlier; ControlLogix controllers 20 and earlier; GuardLogix controllers 20 and earlier; and MicroLogix 1100 and 1400 allows remote attackers to cause a denial of service (CPU crash and communication outage) via a malformed CIP packet.



**10.48.1.100**  
10.48.1.100


**ROCKWELL AUTOMATION**

Security Score 32%

★ 1 Unacknowledged Alert exists

## Most Severe CVE

CVE ID	Score	Description
CVE-2020-6990	10.0	Rockwell Automation MicroLogix 1400 Controllers Series B v21.001 and prior, Series A, all versions, MicroLogix 1100 Controller, all versions, RSLogix 500 Software v12.001 and prior, The cryptographic key utilized to help protect the account password is hard coded into the RSLogix 500 binary file. An attacker could identify cryptographic keys and use it for further cryptographic attacks that could ultimately lead to a remote attacker gaining unauthorized access to the controller.
CVE-2012-6437	10.0	Rockwell Automation EtherNet/IP products; 1756-ENBT, 1756-EWEB, 1768-ENBT, and 1768-EWEB communication modules; CompactLogix L32E and L35E controllers; 1788-ENBT FLEXLogix adapter; 1794-AENTR FLEX I/O EtherNet/IP adapter; ControlLogix 18 and earlier; CompactLogix 18 and earlier; GuardLogix 18 and earlier; SoftLogix 18 and earlier; CompactLogix controllers 19 and earlier; SoftLogix controllers 19 and earlier; ControlLogix controllers 20 and earlier; GuardLogix controllers 20 and earlier; and MicroLogix 1100 and 1400 do not properly perform authentication for Ethernet firmware updates, which allows remote attackers to execute arbitrary code via a Trojan horse update image.
CVE-2015-6490	10.0	Stack-based buffer overflow on Allen-Bradley MicroLogix 1100 devices before B FRN 15.000 and 1400 devices through B FRN 15.003 allows remote attackers to execute arbitrary code via unspecified vectors.
CVE-2012-6440	9.3	The web-server password-authentication functionality in Rockwell Automation EtherNet/IP products; 1756-ENBT, 1756-EWEB, 1768-ENBT, and 1768-EWEB communication modules; CompactLogix L32E and L35E controllers; 1788-ENBT FLEXLogix adapter; 1794-AENTR FLEX I/O EtherNet/IP adapter; ControlLogix 18 and earlier; CompactLogix 18 and earlier; GuardLogix 18 and earlier; SoftLogix 18 and earlier; CompactLogix controllers 19 and earlier; SoftLogix controllers 19 and earlier; ControlLogix controllers 20 and earlier; GuardLogix controllers 20 and earlier; and MicroLogix 1100 and 1400 allows man-in-the-middle attackers to conduct replay attacks via HTTP traffic.
CVE-2012-6439	8.5	Rockwell Automation EtherNet/IP products; 1756-ENBT, 1756-EWEB, 1768-ENBT, and 1768-EWEB communication modules; CompactLogix L32E and L35E controllers; 1788-ENBT FLEXLogix adapter; 1794-AENTR FLEX I/O EtherNet/IP adapter; ControlLogix 18 and earlier; CompactLogix 18 and earlier; GuardLogix 18 and earlier; SoftLogix 18 and earlier; CompactLogix controllers 19 and earlier; SoftLogix controllers 19 and earlier; ControlLogix controllers 20 and earlier; GuardLogix controllers 20 and earlier; and MicroLogix 1100 and 1400 allow remote attackers to cause a denial of service (control and communication outage) via a CIP message that modifies the (1) configuration or (2) network parameters.


**10.1.2.1**  
10.1.2.1

**RUGGEDCOM INC.**

**Security Score** 32%


## ★ 1 Unacknowledged Alert exists

### Ports In Use

- TCP PORT 44818 (Ethernet/IP)

### Most Severe CVE

CVE ID	Score	Description
CVE-2018-17924	7.8	Rockwell Automation MicroLogix 1400 Controllers and 1756 ControlLogix Communications Modules An unauthenticated, remote threat actor could send a CIP connection request to an affected device, and upon successful connection, send a new IP configuration to the affected device even if the controller in the system is set to Hard RUN mode. When the affected device accepts this new IP configuration, a loss of communication occurs between the device and the rest of the system as the system traffic is still attempting to communicate with the device via the overwritten IP address.
CVE-2016-9343	7.5	An issue was discovered in Rockwell Automation Logix5000 Programmable Automation Controller FRN 16.00 through 21.00 (excluding all firmware versions prior to FRN 16.00, which are not affected). By sending malformed common industrial protocol (CIP) packet, an attacker may be able to overflow a stack-based buffer and execute code on the controller or initiate a nonrecoverable fault resulting in a denial of service.
CVE-2019-12262	7.5	Wind River VxWorks 6.6, 6.7, 6.8, 6.9 and 7 has Incorrect Access Control in the RARP client component. IPNET security vulnerability: Handling of unsolicited Reverse ARP replies (Logical Flaw).
CVE-2019-12255	7.5	Wind River VxWorks has a Buffer Overflow in the TCP component (issue 1 of 4). This is a IPNET security vulnerability: TCP Urgent Pointer = 0 that leads to an integer underflow.
CVE-2019-12256	7.5	Wind River VxWorks 6.9 and vx7 has a Buffer Overflow in the IPv4 component. There is an IPNET security vulnerability: Stack overflow in the parsing of IPv4 packets' IP options.



**192.168.90.105**  
192.168.90.105

**UNIVERSAL GLOBAL SCIENTIFIC INDUSTRIAL CO. LTD.**

**Security Score** 35%

## ★ Scanning network devices periodically

## ★ 2 Unacknowledged Alerts exist


**192.168.90.12**  
192.168.90.12

**HEWLETT PACKARD**

**Security Score** 35%

## ★ 1 Unacknowledged Alert exists

### Ports In Use







- TCP PORT 21 (FTP)
- UDP PORT 123 (Network Time Protocol)

### Remote Access

- TCP port 22 (SSH) Connections from 192.168.90.250

### Weak Authentication - Plain text passwords

- Password: c\*\*\*\*\*  
Strength: Medium  
Protocol: FTP

	192.168.92.30 192.168.92.30	INTEL CORPORATE	Security Score 35%
<div data-bbox="172 407 571 436">★ 3 Unacknowledged Alerts exist</div>			
	192.168.90.109 192.168.90.109	LCFC(HEFEI) ELECTRONICS TECHNOLOGY CO. LTD.	Security Score 35%
<div data-bbox="172 573 571 602">★ 2 Unacknowledged Alerts exist</div> <div data-bbox="172 624 319 651">Ports In Use</div> <div data-bbox="181 665 368 689">○ TCP PORT 2869</div>			
	172.19.230.189 172.19.230.189	MICROSOFT CORPORATION	Security Score 35%
<div data-bbox="172 835 571 864">★ 3 Unacknowledged Alerts exist</div> <div data-bbox="172 887 319 913">Ports In Use</div> <div data-bbox="181 927 612 1025"> <div data-bbox="181 927 496 952">○ TCP PORT 445 (SMB over IP)</div> <div data-bbox="181 963 612 987">○ TCP PORT 139 (Netbios Session Service)</div> <div data-bbox="181 999 588 1025">○ TCP PORT 135 (RPC Endpoint Mapper)</div> </div>			
	192.168.66.235 192.168.66.235	VMWARE INC.	Security Score 35%
<div data-bbox="172 1167 571 1196">★ 3 Unacknowledged Alerts exist</div>			
	KOOKY2 172.29.0.111	PCS SYSTEMTECHNIK GMBH	Security Score 40%
<div data-bbox="172 1332 571 1361">★ 1 Unacknowledged Alert exists</div>			
	10.150.90.250 10.150.90.250	PALO ALTO NETWORKS	Security Score 40%
<div data-bbox="172 1500 571 1529">★ 1 Unacknowledged Alert exists</div>			

## Network Security Risks

### Industrial Malware Indicators

Detected during last 30 days

Detection Time	Alert Message	Description	Devices
13/05/2021 13:44:41	Suspicion of Malicious Activity (BlackEnergy)	Suspicious network activity was detected. Such behavior might be attributed to the BlackEnergy malware.	Internet
13/05/2021 13:44:41	Suspicion of Malicious Activity (BlackEnergy)	Suspicious network activity was detected. Such behavior might be attributed to the BlackEnergy malware.	Internet
13/05/2021 13:44:41	Suspicion of Malicious Activity (BlackEnergy)	Suspicious network activity was detected. Such behavior might be attributed to the BlackEnergy malware.	Internet
13/05/2021 13:44:42	Suspicion of Malicious Activity	Suspicious network activity was detected from source 192.168.1.88 to destination 192.168.1.2 on port 1502. This behavior might be attributed to Triton malware.	192.168.1.2, 192.168.1.88
13/05/2021 13:44:45	Invalid SMB Message (DoublePulsar Backdoor Implant)	An invalid SMB message was sent. The message indicates usage of a DoublePulsar backdoor implant. DoublePulsar enables the execution of additional malicious code, for example WannaCry ransomware attacks. Source 10.2.1.3 sent an invalid SMB message to destination 10.2.1.12.	10.2.1.3
13/05/2021 13:44:45	Suspicion of NotPetya Malware - Illegal SMB Transaction Detected	A suspicious SMB message was sent from client 10.2.1.3 to server 10.2.1.12. This message includes a sequence of transaction commands, using a specific combination of command types (NT TRANSACTION, TRANSACTION 2), which is considered illegal. This protocol behavior can be a part of an attack, using Windows exploits such as EternalBlue or EternalRomance, used by WannaCry and NotPetya malwares.	10.2.1.3
13/05/2021 13:45:17	Port Scan Detected	Port scan detected. Scanning device: 192.168.90.105 Scanned device: 192.168.90.112 Scanned Ports: 1900, 20000, 20005, 2160, 2161, 3001, 3003, 3005, 3006, 3007... It is recommended to notify the security officer of the incident.	192.168.90.105
13/05/2021 13:45:31	Suspicion of Malicious Activity (Poison Ivy)	Suspicious network activity was detected. Such behavior might be attributed to the Poison Ivy malware.	10.0.0.1
13/05/2021 13:45:36	Invalid SMB Message (DoublePulsar Backdoor Implant)	An invalid SMB message was sent. The message indicates usage of a DoublePulsar backdoor implant. DoublePulsar enables the execution of additional malicious code, for example WannaCry ransomware attacks. Source 192.168.92.30 sent an invalid SMB message to destination 192.168.92.31.	192.168.92.30
13/05/2021 13:45:36	Suspicion of NotPetya Malware - Illegal SMB Transaction Detected	A suspicious SMB message was sent from client 192.168.92.30 to server 192.168.92.31. This message includes a sequence of transaction commands, using a specific combination of command types (NT TRANSACTION, TRANSACTION 2), which is considered illegal. This protocol behavior can be a part of an attack, using Windows exploits such as EternalBlue or EternalRomance, used by WannaCry and NotPetya malwares.	192.168.92.30
13/05/2021 13:46:17	Port Scan Detected	Port scan detected. Scanning device: 172.19.227.216 Scanned device: 172.19.230.189 Scanned Ports: 10004, 1074, 1287, 139, 15003, 15660, 1583, 16113, 1688, 1720... It is recommended to notify the security officer of the incident.	172.19.227.216

## Weak Firewall Rules

No firewall data was defined in the console. Unable to analyze firewall policies

## Unauthorized Devices

Current unauthorized devices

Address	Name	First Detection Time	Last Seen
No data found			

## Internet Connections

Internal Address	Authorized	External Addresses
10.10.10.25	Yes	8.8.8.8
10.150.90.129	Yes	34.226.68.35 , 54.144.111.231 , 64.74.103.155
10.150.90.250	Yes	199.167.52.141 , 54.225.164.101 , 54.243.77.59
172.19.230.189	Yes	51.104.166.192
172.29.0.111	Yes	68.87.71.230 , 68.87.73.246
192.168.0.107	Yes	144.208.124.152 , 198.54.117.211 , 198.54.117.216
192.168.66.235	Yes	166.161.16.230
192.168.90.10	Yes	207.234.209.181
192.168.90.105	Yes	8.8.8.8
192.168.90.109	Yes	157.56.176.213 , 173.193.174.199 , 173.194.65.188 , 212.179.17.163 , 216.58.198.238 , 216.58.213.99 , 216.58.214.46 , 23.53.50.135 , 66.235.148.140 , 81.218.16.237 , 81.218.16.251
192.168.90.12	Yes	66.22.111.2
192.168.92.30	Yes	8.8.8.8

## Illegal Traffic by Firewall Rules

No firewall data was defined in the console. Unable to analyze firewall policies



## Access Points

MAC Address	Vendor	IP Address	Name	Wireless
00:19:5b:59:20:a0	D-LINK CORPORATION	192.168.90.100	192.168.90.100	Yes
6c:f3:7f:c1:a2:2b	ARUBA A HEWLETT PACKARD ENTERPRISE COMPANY	10.150.90.6	10.150.90.6	Yes
00:18:f8:6f:ac:09	CISCO-LINKSYS LLC	N/A	N/A	Suspected
00:19:5b:59:20:a0	D-LINK CORPORATION	192.168.90.100	192.168.90.100	Suspected
00:22:b0:05:01:01	D-LINK CORPORATION	192.168.20.8	192.168.20.8	Suspected
14:cc:20:ef:b8:4e	TP-LINK TECHNOLOGIES CO.LTD.	192.168.90.253	192.168.90.253	Suspected
2c:3a:fd:a7:8c:ea	AVM AUDIOVISUELLES MARKETING UND COMPUTERSYSTEME GMBH	N/A	N/A	Suspected
00:0c:29:62:f1:48	VMWARE INC.	N/A	N/A	No
00:0c:29:6e:60:fe	VMWARE INC.	N/A	N/A	No
00:0d:65:7b:cc:00	CISCO SYSTEMS INC	N/A	N/A	No
00:15:5d:c1:16:ae	MICROSOFT CORPORATION	N/A	N/A	No
08:5b:0e:46:1b:ec	FORTINET INC.	N/A	N/A	No
08:5b:0e:a1:df:9e	FORTINET INC.	N/A	N/A	No
b4:0c:25:bc:cf:11	PALO ALTO NETWORKS	N/A	N/A	No
c8:d3:ff:12:33:21	HEWLETT PACKARD	192.168.90.250	192.168.90.250	No



## Connections to ICS networks

The following are cross ICS subnet connections. Verify that these connections are authorized.

ICS Subnet	Connected Subnet
10.1.1.0/24	10.10.5.0/24
10.1.2.0/24	10.2.0.0/24
10.10.3.0/24	192.168.159.0/24
10.10.5.0/24	10.1.1.0/24
10.2.0.0/24	10.1.2.0/24
10.4.0.0/24	10.4.2.0/24, 10.5.0.0/24, 10.5.2.0/24
10.4.2.0/24	10.4.0.0/24
10.5.0.0/24	10.4.0.0/24
10.5.2.0/24	10.4.0.0/24
10.92.18.0/24	192.168.1.0/24
172.16.0.0/24	172.16.1.0/24
172.16.1.0/24	172.16.0.0/24
192.168.1.0/24	10.92.18.0/24, 192.168.2.0/24
192.168.10.0/24	192.168.100.0/24, 192.168.90.0/24
192.168.159.0/24	10.10.3.0/24
192.168.160.0/24	192.168.90.0/24
192.168.2.0/24	192.168.1.0/24
192.168.20.0/24	192.168.90.0/24
192.168.30.0/24	192.168.90.0/24
192.168.40.0/24	192.168.90.0/24
192.168.90.0/24	10.10.10.0/24, 192.168.10.0/24, 192.168.160.0/24, 192.168.20.0/24, 192.168.30.0/24, 192.168.40.0/24, 192.168.60.0/24, 192.168.92.0/24, Unclassified Subnet (336 connections)

## Network Operations

### Protocol Problems

Detected during last 30 days

Protocol	Alert	Report Time	Addresses
RPC	RPC Operation Failed	13/05/2021 13:45:38	192.168.40.3, 192.168.90.20
RPC	RPC Operation Failed	13/05/2021 13:45:38	192.168.60.16, 192.168.90.20
RPC	RPC Operation Failed	13/05/2021 13:45:37	192.168.30.1, 192.168.90.20
RPC	RPC Operation Failed	13/05/2021 13:45:36	192.168.10.1, 192.168.90.20
RPC	RPC Operation Failed	13/05/2021 13:45:36	192.168.20.1, 192.168.90.20
SMB	Invalid SMB Message (DoublePulsar Backdoor Implant)	13/05/2021 13:45:36	192.168.92.31, 192.168.92.30
SMB	Suspicion of NotPetya Malware - Illegal SMB Transaction Detected	13/05/2021 13:45:36	192.168.92.31, 192.168.92.30
SMB	Invalid SMB Message (DoublePulsar Backdoor Implant)	13/05/2021 13:44:45	10.2.1.3, 10.2.1.12
SMB	Suspicion of NotPetya Malware - Illegal SMB Transaction Detected	13/05/2021 13:44:45	10.2.1.3, 10.2.1.12
SRTP	GE SRTP Stop PLC Command was Sent	13/05/2021 13:44:46	192.168.90.109, 192.168.90.62
DNP3	Outstation Restarts Frequently	13/05/2021 13:45:02	192.168.30.4
DNP3	Outstation Restarted	13/05/2021 13:44:45	192.168.30.4, 192.168.30.3
DNP3	Illegal DNP3 Operation	13/05/2021 13:44:45	192.168.30.4, 192.168.30.3
DNP3	Master-Slave Authentication Error	13/05/2021 13:44:45	192.168.30.4, 192.168.30.3
DNP3	Outstation's Configuration Changed	13/05/2021 13:44:45	192.168.30.4, 192.168.30.3
DNP3	Outstation's Corrupted Configuration Detected	13/05/2021 13:44:45	192.168.30.1, 192.168.30.3
DNP3	Illegal DNP3 Operation	13/05/2021 13:44:45	192.168.30.4, 192.168.30.3
DNP3	Suspicion of Hardware Problems in Outstation	13/05/2021 13:44:45	192.168.30.1, 192.168.30.3
DNP3	Incorrect Parameter Sent to Outstation	13/05/2021 13:44:45	192.168.30.1, 192.168.30.2
DNP3	Outstation Restarted	13/05/2021 13:44:45	192.168.30.4, 192.168.30.2
ETHERNET/IP	EtherNet/IP CIP Service Request Failed	13/05/2021 13:48:22	10.1.2.1, 10.2.0.53
ETHERNET/IP	EtherNet/IP Encapsulation Protocol Command Failed	13/05/2021 13:48:21	10.48.1.100
ETHERNET/IP	EtherNet/IP CIP Service Request Failed	13/05/2021 13:46:53	192.168.100.37, 192.168.100.28
ETHERNET/IP	EtherNet/IP Encapsulation Protocol Command Failed	13/05/2021 13:46:53	192.168.20.5, 192.168.20.8
ETHERNET/IP	EtherNet/IP Encapsulation Protocol Command Failed	13/05/2021 13:46:53	10.92.18.100, 10.92.18.17
ETHERNET/IP	EtherNet/IP CIP Service Request Failed	13/05/2021 13:46:53	192.168.100.28, 192.168.100.36
ETHERNET/IP	EtherNet/IP Encapsulation Protocol Command Failed	13/05/2021 13:46:53	10.92.18.100, 10.92.18.17
ETHERNET/IP	EtherNet/IP CIP Service Request Failed	13/05/2021 13:46:53	192.168.100.28, 192.168.100.36
ETHERNET/IP	EtherNet/IP CIP Service Request Failed	13/05/2021 13:46:53	192.168.100.28, 192.168.100.36
ETHERNET/IP	EtherNet/IP Encapsulation Protocol Command Failed	13/05/2021 13:46:53	10.92.18.100, 10.92.18.17
ETHERNET/IP	EtherNet/IP CIP Service Request Failed	13/05/2021 13:45:37	192.168.110.11, 192.168.110.6

Protocol	Alert	Report Time	Addresses
MMS	MMS Service Request Failed	13/05/2021 13:45:36	172.16.0.73, 172.16.1.1
MODBUS	Suspicion of Unresponsive MODBUS Device	13/05/2021 13:46:49	
MODBUS	Modbus Exception	13/05/2021 13:46:32	192.168.109.1, 192.168.109.20
MODBUS	Modbus Exception	13/05/2021 13:46:32	10.2.1.43, 10.2.1.22
MODBUS	Modbus Exception	13/05/2021 13:46:32	10.0.0.3, 10.0.0.57
MODBUS	Modbus Exception	13/05/2021 13:46:32	192.168.66.235, 166.161.16.230
MODBUS	Modbus Exception	13/05/2021 13:46:32	192.168.66.235, 166.161.16.230
MODBUS	Modbus Exception	13/05/2021 13:46:22	10.141.30.50
SIEMENS-S7	An S7 Stop PLC Command was Sent	13/05/2021 13:46:53	192.168.1.1, 192.168.2.2
SIEMENS-S7	An S7 Stop PLC Command was Sent	13/05/2021 13:44:45	192.168.10.1, 192.168.10.3

## Protocol Data Volumes

Top 20 from last 24 hours

Protocol	Volume
DHCP (67)	0.511 MB

## Disconnections

Detected during last 30 days

Device Address	Device Name	Last Detection Time	Back to Normal Time
192.168.90.112	192.168.90.112	13/05/2021 13:45:44	N/A
172.19.230.189	172.19.230.189	13/05/2021 13:46:44	N/A

## Backup server

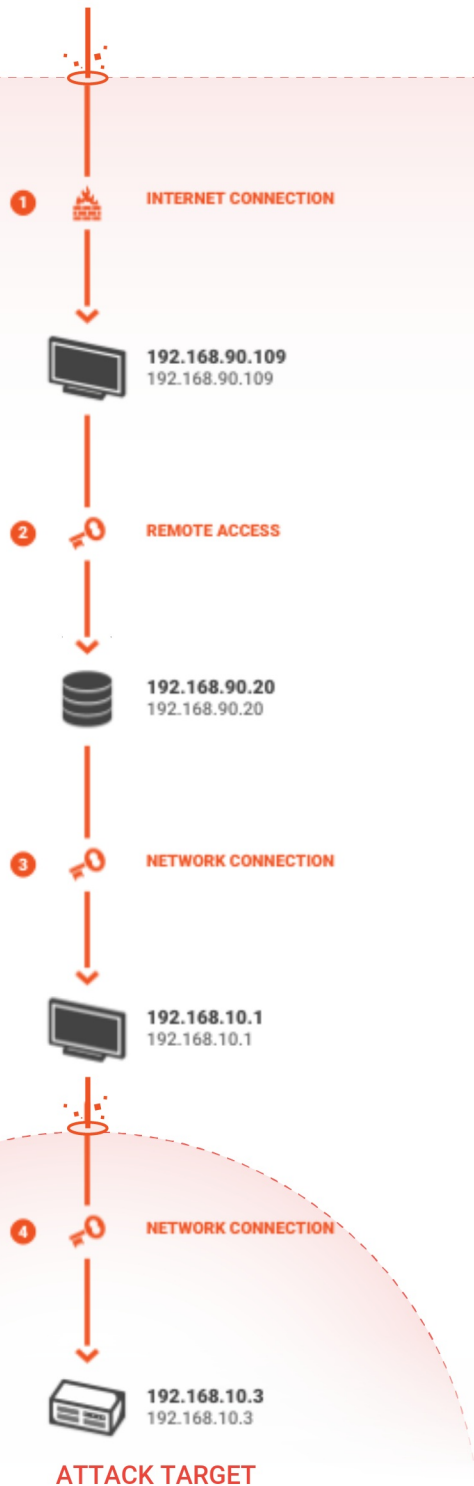
No operating Backup servers were detected

## IP Networks

Network	Mask	Name	Addresses
192.168.90.0	255.255.255.0	N/A	39
172.18.32.0	255.255.255.0	N/A	17
192.168.10.0	255.255.255.0	N/A	17
10.10.10.0	255.255.255.0	N/A	9
10.150.90.0	255.255.255.0	N/A	9
192.168.107.0	255.255.255.0	N/A	7
192.168.100.0	255.255.255.0	N/A	7
192.168.20.0	255.255.255.0	N/A	6
10.0.0.0	255.255.255.0	N/A	5
192.168.92.0	255.255.255.0	N/A	5
10.2.1.0	255.255.255.0	N/A	4

Network	Mask	Name	Addresses
192.168.30.0	255.255.255.0	N/A	4
192.168.1.0	255.255.255.0	N/A	4
192.168.40.0	255.255.255.0	N/A	4
10.92.18.0	255.255.255.0	N/A	3
10.141.30.0	255.255.255.0	N/A	3
10.140.100.0	255.255.255.0	N/A	3
10.1.93.0	255.255.255.0	N/A	2
10.4.0.0	255.255.255.0	N/A	2
192.168.110.0	255.255.255.0	N/A	2
10.5.2.0	255.255.255.0	N/A	2
192.168.109.0	255.255.255.0	N/A	2
10.1.1.0	255.255.255.0	N/A	2
10.1.80.0	255.255.255.0	N/A	2
172.29.0.0	255.255.255.0	N/A	2
192.168.0.0	255.255.255.0	N/A	2
172.19.230.0	255.255.255.0	N/A	1
10.2.0.0	255.255.255.0	N/A	1
10.10.3.0	255.255.255.0	N/A	1
10.1.85.0	255.255.255.0	N/A	1
10.1.10.0	255.255.255.0	N/A	1
10.5.0.0	255.255.255.0	N/A	1
192.168.159.0	255.255.255.0	N/A	1
10.140.10.0	255.255.255.0	N/A	1
10.142.1.0	255.255.255.0	N/A	1
172.16.1.0	255.255.255.0	N/A	1
192.168.60.0	255.255.255.0	N/A	1
10.1.76.0	255.255.255.0	N/A	1
192.168.66.0	255.255.255.0	N/A	1
10.1.84.0	255.255.255.0	N/A	1
10.4.2.0	255.255.255.0	N/A	1
192.168.2.0	255.255.255.0	N/A	1
10.1.73.0	255.255.255.0	N/A	1
10.1.2.0	255.255.255.0	N/A	1
192.168.160.0	255.255.255.0	N/A	1
10.1.88.0	255.255.255.0	N/A	1
172.16.0.0	255.255.255.0	N/A	1

Network	Mask	Name	Addresses
10.1.72.0	255.255.255.0	N/A	1
10.48.1.0	255.255.255.0	N/A	1
10.10.5.0	255.255.255.0	N/A	1
172.19.227.0	255.255.255.0	N/A	1
172.19.224.0	255.255.255.0	N/A	1



## Attack Vector #1

### (1) Internet Connection

192.168.90.109 is exposed to external threats due to internet connectivity

### (2) Remote Access

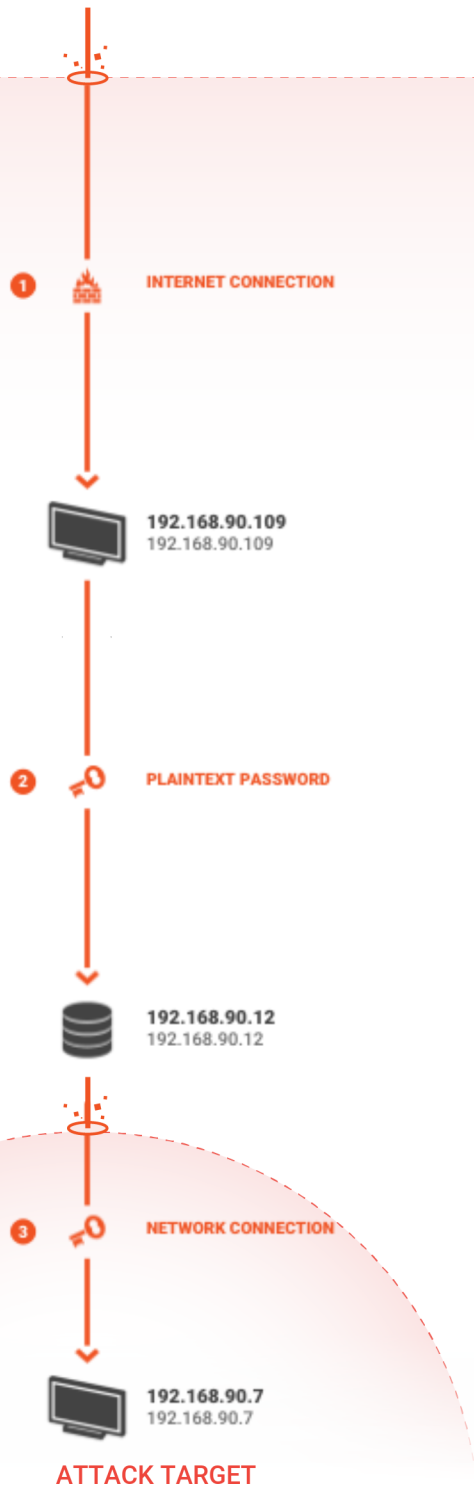
Allowed remote access using TeamViewer

### (3) Network Connection

Direct connection between devices located in different subnets

### (4) Network Connection

Direct connection between devices



## Attack Vector #2

### (1) Internet Connection

192.168.90.109 is exposed to external threats due to internet connectivity

### (2) Plaintext Password

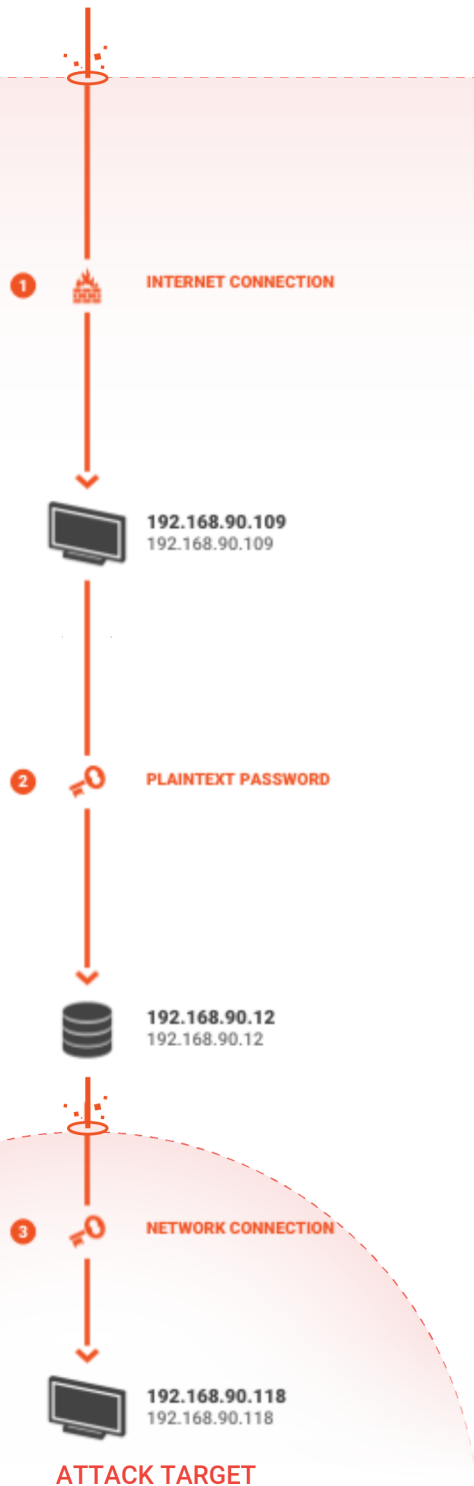
Device 192.168.90.12 can be accessed using plaintext password c\*\*\*\*\*, for FTP authentication.

An attacker could extract this password from the network traffic

This server can be used by the attacker to persist malware in the network

### (3) Network Connection

Direct connection between devices



## Attack Vector #3

### (1) Internet Connection

192.168.90.109 is exposed to external threats due to internet connectivity

### (2) Plaintext Password

Device 192.168.90.12 can be accessed using plaintext password c\*\*\*\*\*, for FTP authentication.

An attacker could extract this password from the network traffic

This server can be used by the attacker to persist malware in the network

### (3) Network Connection

Direct connection between devices



## Mitigation

Please note, the following enhancements are available:

- ★ Firewall policy import
- ★ Further device information import

☐ Check any Internet Connections ensuring all are allowed. Consider removing unnecessary connections or using an offline-proxy or a Unidirectional Security Gateway **14%** Maximum Security Impact

Internal Address	Authorized	External Addresses
10.10.10.25	Yes	8.8.8.8
10.150.90.129	Yes	34.226.68.35 , 54.144.111.231 , 64.74.103.155
10.150.90.250	Yes	199.167.52.141 , 54.225.164.101 , 54.243.77.59
172.19.230.189	Yes	51.104.166.192
172.29.0.111	Yes	68.87.71.230 , 68.87.73.246
192.168.0.107	Yes	144.208.124.152 , 198.54.117.211 , 198.54.117.216
192.168.66.235	Yes	166.161.16.230
192.168.90.10	Yes	207.234.209.181
192.168.90.105	Yes	8.8.8.8
192.168.90.109	Yes	157.56.176.213 , 173.193.174.199 , 173.194.65.188 , 212.179.17.163 , 216.58.198.238 , 216.58.213.99 , 216.58.214.46 , 23.53.50.135 , 66.235.148.140 , 81.218.16.237 , 81.218.16.251
192.168.90.12	Yes	66.22.111.2
192.168.92.30	Yes	8.8.8.8

☐ Upgrade firmware to the latest version (Devices: 6) **12%** Maximum Security Impact

Name	Address
10.48.1.100	10.48.1.100
192.168.10.120	192.168.10.120
192.168.10.3	192.168.10.3
192.168.10.4	192.168.10.4
192.168.110.6	192.168.110.6
192.168.90.122	192.168.90.122

☐ Install an Antivirus solution to increase protection of the workstations **10%** Maximum Security Impact

☐ Investigate all malware indicators (Contact your incident response team or support.microsoft.com). When assured the problem is solved, acknowledge the alert 7% Maximum Security Impact

Detection Time	Alert Message	Description	Devices
13/05/2021 13:44:41	Suspicion of Malicious Activity (BlackEnergy)	Suspicious network activity was detected. Such behavior might be attributed to the BlackEnergy malware.	Internet
13/05/2021 13:44:41	Suspicion of Malicious Activity (BlackEnergy)	Suspicious network activity was detected. Such behavior might be attributed to the BlackEnergy malware.	Internet
13/05/2021 13:44:41	Suspicion of Malicious Activity (BlackEnergy)	Suspicious network activity was detected. Such behavior might be attributed to the BlackEnergy malware.	Internet
13/05/2021 13:44:42	Suspicion of Malicious Activity	Suspicious network activity was detected from source 192.168.1.88 to destination 192.168.1.2 on port 1502. This behavior might be attributed to Triton malware.	192.168.1.2, 192.168.1.88
13/05/2021 13:44:45	Invalid SMB Message (DoublePulsar Backdoor Implant)	An invalid SMB message was sent. The message indicates usage of a DoublePulsar backdoor implant. DoublePulsar enables the execution of additional malicious code, for example WannaCry ransomware attacks. Source 10.2.1.3 sent an invalid SMB message to destination 10.2.1.12.	10.2.1.3
13/05/2021 13:44:45	Suspicion of NotPetya Malware - Illegal SMB Transaction Detected	A suspicious SMB message was sent from client 10.2.1.3 to server 10.2.1.12. This message includes a sequence of transaction commands, using a specific combination of command types (NT TRANSACTION, TRANSACTION 2), which is considered illegal. This protocol behavior can be a part of an attack, using Windows exploits such as EternalBlue or EternalRomance, used by WannaCry and NotPetya malwares.	10.2.1.3
13/05/2021 13:45:17	Port Scan Detected	Port scan detected. Scanning device: 192.168.90.105 Scanned device: 192.168.90.112 Scanned Ports: 1900, 20000, 20005, 2160, 2161, 3001, 3003, 3005, 3006, 3007... It is recommended to notify the security officer of the incident.	192.168.90.105
13/05/2021 13:45:31	Suspicion of Malicious Activity (Poison Ivy)	Suspicious network activity was detected. Such behavior might be attributed to the Poison Ivy malware.	10.0.0.1
13/05/2021 13:45:36	Invalid SMB Message (DoublePulsar Backdoor Implant)	An invalid SMB message was sent. The message indicates usage of a DoublePulsar backdoor implant. DoublePulsar enables the execution of additional malicious code, for example WannaCry ransomware attacks. Source 192.168.92.30 sent an invalid SMB message to destination 192.168.92.31.	192.168.92.30
13/05/2021 13:45:36	Suspicion of NotPetya Malware - Illegal SMB Transaction Detected	A suspicious SMB message was sent from client 192.168.92.30 to server 192.168.92.31. This message includes a sequence of transaction commands, using a specific combination of command types (NT TRANSACTION, TRANSACTION 2), which is considered illegal. This protocol behavior can be a part of an attack, using Windows exploits such as EternalBlue or EternalRomance, used by WannaCry and NotPetya malwares.	192.168.92.30
13/05/2021 13:46:17	Port Scan Detected	Port scan detected. Scanning device: 172.19.227.216 Scanned device: 172.19.230.189 Scanned Ports: 10004, 1074, 1287, 139, 15003, 15660, 1583, 16113, 1688, 1720... It is recommended to notify the security officer of the incident.	172.19.227.216

☐ Install a backup server in the network 5% Maximum Security Impact

☐ Investigate and acknowledge all unacknowledge alerts 4% Maximum Security Impact

Detection Time	Alert Message	Description
13/05/2021 13:45:36	Suspicion of NotPetya Malware - Illegal SMB Transaction Detected	A suspicious SMB message was sent from client 192.168.92.30 to server 192.168.92.31. This message includes a sequence of transaction commands, using a specific combination of command types (NT TRANSACTION, TRANSACTION 2), which is considered illegal. This protocol behavior can be a part of an attack, using Windows exploits such as EternalBlue or EternalRomance, used by WannaCry and NotPetya malwares.
13/05/2021 13:44:45	Suspicion of NotPetya Malware - Illegal SMB Transaction Detected	A suspicious SMB message was sent from client 10.2.1.3 to server 10.2.1.12. This message includes a sequence of transaction commands, using a specific combination of command types (NT TRANSACTION, TRANSACTION 2), which is considered illegal. This protocol behavior can be a part of an attack, using Windows exploits such as EternalBlue or EternalRomance, used by WannaCry and NotPetya malwares.
13/05/2021 13:47:55	Unauthorized Internet Connectivity Detected	A device defined in your internal network is communicating with addresses on the Internet. These addresses have not been learned as valid addresses. Device 192.168.90.109 communicated with addresses shown in External Addresses. Verify that this device is properly configured.

☐ Install latest security updates (Devices: 9) 1% Maximum Security Impact

Name	Address
10.1.1.164	10.1.1.164
10.1.2.1	10.1.2.1
192.168.10.15	192.168.10.15
192.168.159.123	192.168.159.123
192.168.90.250	192.168.90.250
192.168.90.251	192.168.90.251
DESKTOP-NRNGSEK	192.168.90.117
HOBARTRANCH764	10.150.90.129
USER-PC	192.168.1.1

☐ Consider installing a more recent operating system version, which has continuous security updates, (Devices: 1) 1% Maximum Security Impact

Name	Address
10.10.10.25	10.10.10.25

☐ Use passwords for authentication (Devices: 1) 1% Maximum Security Impact

Name	Address
172.16.1.1	172.16.1.1

☐ Increase password complexity for authentication (Devices: 4) 1% Maximum Security Impact

Name	Address
192.168.10.11	192.168.10.11
192.168.90.100	192.168.90.100
192.168.90.12	192.168.90.12
192.168.92.130	192.168.92.130