Confidential Document

VULNERABILITY DISCOVERY SERVICE
Critical Findings Report

Prepared for

INSERT CUSTOMER LOGO HERE

Spacely Sprockets

Mikwaukee, WI

Demo Facility 1

RA Document: 9300-VDS-0001

Project Number: 001

11/29/2023

Version 1 Revision 0

INSERT ASP LOGO HERE

Rockwell Automation

Spacely Sprockets – Mikwaukee, WI
VULNERABILITY DISCOVERY SERVICE
CONTENTS

1 DOCUMENT CONTROL **3**

1.1 Document Approval 3
1.2 Revision History 3
1.3 Disclaimer 3

2 BACKGROUND & OVERVIEW **4**

2.1 Executive Summary 4
2.2 Project Goals 5
2.3 Key Findings 5

3 DATA COLLECTION INFORMATION **22**

4 SUMMARY OF SURVEY FINDINGS **24**

4.1 Device Communication Statistics 25
4.2 Asset Identification 26

INSERT ASP LOGO HERE

Rockwell Automation

Spacely Sprockets – Mikwaukee, WI
VULNERABILITY DISCOVERY SERVICE
Figure & Tables

Table 1:1 – Document Approval 3
Table 1:2 – Revision History 3
Figure 2:1 – Vulnerability Discovery Improvement Plan 4
Table 2:1 – Device Vulnerabilities 6
Table 2:2 – Unsupported Windows Operating Systems 21
Table 3:1 - Scope Qualification Information 22
Table 3:2 - Collection Network Information 23
Table 4:1 - Insights Summary 24
Table 4:2 – Counters 25
Table 4:3 - Asset Distribution by Type 25
Table 4:4 - Asset Vendors 25
Table 4:5 - Connected Asset 26

INSERT ASP LOGO HERE

Rockwell Automation

1 DOCUMENT CONTROL

1.1 Document Approval

Table 1:1 – Document Approval

Date	Organization	Name - Title
11/29/2023	Distributor Company	Jane Doe – Automation Network Engineer
11/29/2023	Rockwell Automation	Steven Taylor - Engineering Team Lead
Pending	Spacely Sprockets	John Doe – Project Engineering Manager

1.2 Revision History

Table 1:2 – Revision History

Date	Version	Description	Author
11/29/2023	v1r0	1st Draft Delivered	Rockwell Automation Authorized Service Provider Program

1.3 Disclaimer

All information contained herein is provided without any warranty, expressed or implied, as to the accuracy or relevance of such information to the Spacely Sprockets, Mikwaukee, WI environment. This information is to be considered as preliminary and informative and is subject to review and revision at any time by Spacely Sprockets, Distributor Company, or Rockwell Automation. This document further includes information that may be proprietary, confidential, or otherwise sensitive to Spacely Sprockets, Distributor Company, and Rockwell Automation. Prior to any dissemination outside of Spacely Sprockets, Distributor Company, or Rockwell Automation of any part or whole of this document, all relevant parties must agree in writing. The information contained herein may be considered volatile and preliminary, subject to revision, addition, or removal.

INSERT ASP LOGO HERE

Rockwell Automation

2 BACKGROUND & OVERVIEW

2.1 Executive Summary

Spacely Sprockets has approved the Rockwell Automation Authorized Service Provider Program to scan strategically selected subnets at this facility for the purpose of discovering security vulnerabilities of assets and applications on the network. The Vulnerability Discovery Service has been developed to use active network methods to provide a security analysis of the system. These methods are strategically collected using Claroty Edge and analyzed using the Claroty Threat Detection Engine. The data analyzed provides an accurate "snapshot" of the current security status of the facility. This document constitutes the Vulnerability Discovery Service Critical Findings report deliverable, focusing on the most critical vulnerabilities and the most critical devices. The figure below demonstrates the continuous phases for how this reporting can be utilized to improve the security status of the facility's system and prioritize the remediation of the most critical weaknesses. Each phase within the overall program cycle is defined in this document.

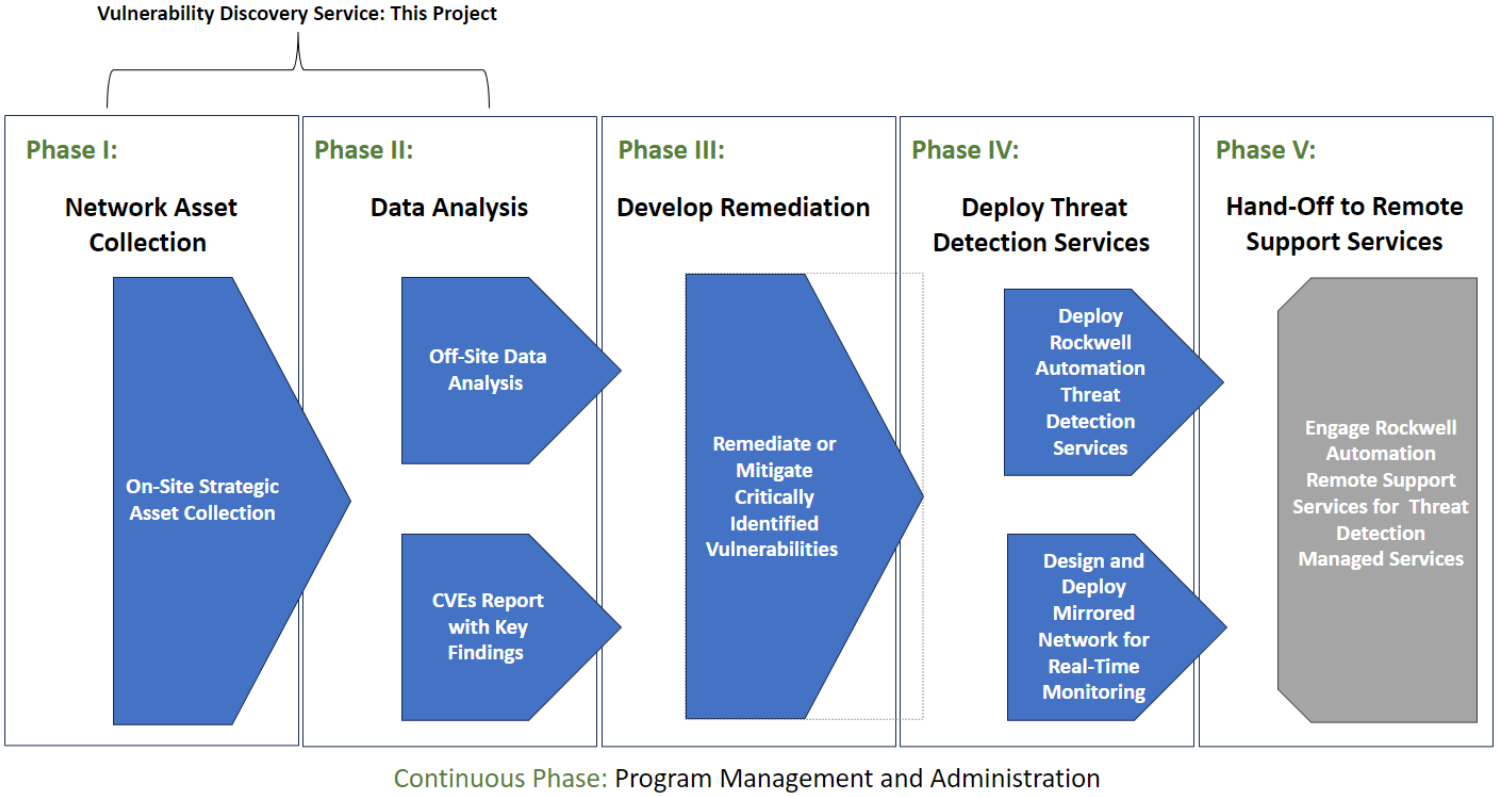

Figure 2:1 – Vulnerability Discovery Improvement Plan

INSERT ASP LOGO HERE

Rockwell Automation

2.2 Project Goals

Perform and deliver an Vulnerability Discovery Service for the desired network segments within the scope of this document on the following pages.

2.3 Key Findings

This section provides an in-depth analysis of all issues which were discovered and attempts to prioritize the most important findings that should be mitigated as soon as possible or that could provide the most risk. Key Findings are identified based on the following categories:

- **Critical Asset Vulnerabilities** – These findings will be based on Critical Assets with vulnerabilities with Critical or High CVE scores.
- **Unsupported Operating Systems** – These findings will be based on any identified end-of-life or no longer patch computer operating system. Will usually be older Windows based desktops or servers.

Note: The Device Vulnerabilities listed in the following table, are based on Common Vulnerability Scoring System (CVSS) scores of between the range of 9.0 - 10. These vulnerabilities will have the following characteristics.

- Remotely Exploitable
- Simple Attack Complexity
- No Privileges Required
- No User Interaction Required
- Confidentially, Integrity, and Available are impacted nearing a complete loss

More information about the CVSS scoring can be found at here.

Only Full Match Vendor CVEs that meet the criticality criteria have been listed. Non-verifiable Vendor Match CVEs have been removed due to the overwhelming quantity of them. The non-verifiable Vendor Match CVEs are still provided in the Comprehensive Data Report in the tab, Vendor Match CVEs.

Table 2:1 – Device Vulnerabilities

Asset	Description	Remediation Guidance
Labeller	RA-58964: CVSS 9.1 - Successful exploitation of this vulnerability could include Denial of Service (DoS)	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/58964
CONT_12	ICSA-19-211-01: CVSS 9.8 - (Urgent/11) Wind River VxWorks Vulnerabilities	https://www.us-cert.gov/ics/advisories/icsa-19-211-01
CONT_09	ICSA-19-211-01: CVSS 9.8 - (Urgent/11) Wind River VxWorks Vulnerabilities	https://www.us-cert.gov/ics/advisories/icsa-19-211-01
CONT_09	ICSA-19-211-01: CVSS 9.8 - (Urgent/11) Wind River VxWorks Vulnerabilities	https://www.us-cert.gov/ics/advisories/icsa-19-211-01
SD59	RA-58964: CVSS 9.1 - Successful exploitation of this vulnerability could include Denial of Service (DoS)	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/58964
CONT_02	ICSA-19-211-01: CVSS 9.8 - (Urgent/11) Wind River VxWorks Vulnerabilities	https://www.us-cert.gov/ics/advisories/icsa-19-211-01
SD59	RA-69735: CVSS 10.0 - Open UDP Port in 1756-ENBT EtherNet/IP Communication Interface	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/69735
10.10.3.1	CVE-2010-5305: CVSS 9.8 - Password exposure by improper access control vulnerability	https://nvd.nist.gov/vuln/detail/CVE-2010-5305
10.10.3.1	RA-511407-2: CVSS 9.1 - The vulnerability in the SLC 500 controller platform occurs when the controller$ Status file property is not set to Static thereby allowing changes to the file contents.	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/511407
10.10.5.25	CVE-2010-5305: CVSS 9.8 - Password exposure by improper access control vulnerability	https://nvd.nist.gov/vuln/detail/CVE-2010-5305
10.10.5.25	RA-511407-2: CVSS 9.1 - The vulnerability in the SLC 500 controller platform occurs when the controller$ Status file property is not set to Static thereby allowing changes to the file contents.	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/511407
10.10.2.31	CVE-2010-5305: CVSS 9.8 - Password exposure by improper access control vulnerability	https://nvd.nist.gov/vuln/detail/CVE-2010-5305
10.10.2.31	RA-511407-2: CVSS 9.1 - The vulnerability in the SLC 500 controller platform occurs when the controller$ Status file property is not set to Static thereby allowing changes to the file contents.	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/511407
10.10.2.25	CVE-2010-5305: CVSS 9.8 - Password exposure by improper access control vulnerability	https://nvd.nist.gov/vuln/detail/CVE-2010-5305

Spacely Sprockets – Mikwaukee, WI
VULNERABILITY DISCOVERY SERVICE

Asset	Description	Remediation Guidance
10.10.2.25	RA-511407-2: CVSS 9.1 - The vulnerability in the SLC 500 controller platform occurs when the controller\uf\uf Status file property is not set to Static thereby allowing changes to the file contents.	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/511407
10.10.3.31	CVE-2010-5305: CVSS 9.8 - Password exposure by improper access control vulnerability	https://nvd.nist.gov/vuln/detail/CVE-2010-5305
10.10.3.31	RA-511407-2: CVSS 9.1 - The vulnerability in the SLC 500 controller platform occurs when the controller\uf\uf Status file property is not set to Static thereby allowing changes to the file contents.	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/511407
10.10.1.25	CVE-2010-5305: CVSS 9.8 - Password exposure by improper access control vulnerability	https://nvd.nist.gov/vuln/detail/CVE-2010-5305
10.10.1.25	RA-511407-2: CVSS 9.1 - The vulnerability in the SLC 500 controller platform occurs when the controller\uf\uf Status file property is not set to Static thereby allowing changes to the file contents.	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/511407
10.10.1.63	CVE-2010-5305: CVSS 9.8 - Password exposure by improper access control vulnerability	https://nvd.nist.gov/vuln/detail/CVE-2010-5305
10.10.1.63	RA-511407-2: CVSS 9.1 - The vulnerability in the SLC 500 controller platform occurs when the controller\uf\uf Status file property is not set to Static thereby allowing changes to the file contents.	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/511407
10.10.2.11	CVE-2010-5305: CVSS 9.8 - Password exposure by improper access control vulnerability	https://nvd.nist.gov/vuln/detail/CVE-2010-5305
10.10.2.11	RA-511407-2: CVSS 9.1 - The vulnerability in the SLC 500 controller platform occurs when the controller\uf\uf Status file property is not set to Static thereby allowing changes to the file contents.	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/511407
10.10.3.61	CVE-2010-5305: CVSS 9.8 - Password exposure by improper access control vulnerability	https://nvd.nist.gov/vuln/detail/CVE-2010-5305
10.10.3.61	RA-511407-2: CVSS 9.1 - The vulnerability in the SLC 500 controller platform occurs when the controller\uf\uf Status file property is not set to Static thereby allowing changes to the file contents.	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/511407
10.10.1.21	CVE-2010-5305: CVSS 9.8 - Password exposure by improper access control vulnerability	https://nvd.nist.gov/vuln/detail/CVE-2010-5305
10.10.1.21	RA-511407-2: CVSS 9.1 - The vulnerability in the SLC 500 controller platform occurs when the controller\uf\uf Status file property is not set to Static thereby allowing changes to the file contents.	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/511407

INSERT ASP LOGO HERE

Rockwell Automation

Spacely Sprockets – Mikwaukee, WI
VULNERABILITY DISCOVERY SERVICE

Asset	Description	Remediation Guidance
10.10.2.61	CVE-2010-5305: CVSS 9.8 - Password exposure by improper access control vulnerability	https://nvd.nist.gov/vuln/detail/CVE-2010-5305
10.10.2.61	RA-511407-2: CVSS 9.1 - The vulnerability in the SLC 500 controller platform occurs when the controller\uf\uf Status file property is not set to Static thereby allowing changes to the file contents.	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/511407
10.10.1.65	CVE-2010-5305: CVSS 9.8 - Password exposure by improper access control vulnerability	https://nvd.nist.gov/vuln/detail/CVE-2010-5305
10.10.1.65	RA-511407-2: CVSS 9.1 - The vulnerability in the SLC 500 controller platform occurs when the controller\uf\uf Status file property is not set to Static thereby allowing changes to the file contents.	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/511407
10.10.2.21	CVE-2010-5305: CVSS 9.8 - Password exposure by improper access control vulnerability	https://nvd.nist.gov/vuln/detail/CVE-2010-5305
10.10.2.21	RA-511407-2: CVSS 9.1 - The vulnerability in the SLC 500 controller platform occurs when the controller\uf\uf Status file property is not set to Static thereby allowing changes to the file contents.	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/511407
10.10.3.23	CVE-2010-5305: CVSS 9.8 - Password exposure by improper access control vulnerability	https://nvd.nist.gov/vuln/detail/CVE-2010-5305
10.10.3.23	RA-511407-2: CVSS 9.1 - The vulnerability in the SLC 500 controller platform occurs when the controller\uf\uf Status file property is not set to Static thereby allowing changes to the file contents.	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/511407
10.10.1.33	CVE-2010-5305: CVSS 9.8 - Password exposure by improper access control vulnerability	https://nvd.nist.gov/vuln/detail/CVE-2010-5305
10.10.1.33	RA-511407-2: CVSS 9.1 - The vulnerability in the SLC 500 controller platform occurs when the controller\uf\uf Status file property is not set to Static thereby allowing changes to the file contents.	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/511407
10.10.3.11	CVE-2010-5305: CVSS 9.8 - Password exposure by improper access control vulnerability	https://nvd.nist.gov/vuln/detail/CVE-2010-5305
10.10.3.11	RA-511407-2: CVSS 9.1 - The vulnerability in the SLC 500 controller platform occurs when the controller\uf\uf Status file property is not set to Static thereby allowing changes to the file contents.	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/511407
10.10.1.61	CVE-2010-5305: CVSS 9.8 - Password exposure by improper access control vulnerability	https://nvd.nist.gov/vuln/detail/CVE-2010-5305

INSERT ASP LOGO HERE

Rockwell Automation

Spacely Sprockets – Mikwaukee, WI
VULNERABILITY DISCOVERY SERVICE

Asset	Description	Remediation Guidance
10.10.1.61	RA-511407-2: CVSS 9.1 - The vulnerability in the SLC 500 controller platform occurs when the controller\uf\uf Status file property is not set to Static thereby allowing changes to the file contents.	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/511407
10.10.11.5	CVE-2010-5305: CVSS 9.8 - Password exposure by improper access control vulnerability	https://nvd.nist.gov/vuln/detail/CVE-2010-5305
10.10.11.5	RA-511407-2: CVSS 9.1 - The vulnerability in the SLC 500 controller platform occurs when the controller\uf\uf Status file property is not set to Static thereby allowing changes to the file contents.	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/511407
10.10.11.3	CVE-2010-5305: CVSS 9.8 - Password exposure by improper access control vulnerability	https://nvd.nist.gov/vuln/detail/CVE-2010-5305
10.10.11.3	RA-511407-2: CVSS 9.1 - The vulnerability in the SLC 500 controller platform occurs when the controller\uf\uf Status file property is not set to Static thereby allowing changes to the file contents.	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/511407
10.10.10.1	CVE-2010-5305: CVSS 9.8 - Password exposure by improper access control vulnerability	https://nvd.nist.gov/vuln/detail/CVE-2010-5305
10.10.10.1	RA-511407-2: CVSS 9.1 - The vulnerability in the SLC 500 controller platform occurs when the controller\uf\uf Status file property is not set to Static thereby allowing changes to the file contents.	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/511407
10.10.3.65	CVE-2010-5305: CVSS 9.8 - Password exposure by improper access control vulnerability	https://nvd.nist.gov/vuln/detail/CVE-2010-5305
10.10.3.65	RA-511407-2: CVSS 9.1 - The vulnerability in the SLC 500 controller platform occurs when the controller\uf\uf Status file property is not set to Static thereby allowing changes to the file contents.	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/511407
10.10.12.1	CVE-2010-5305: CVSS 9.8 - Password exposure by improper access control vulnerability	https://nvd.nist.gov/vuln/detail/CVE-2010-5305
10.10.12.1	RA-511407-2: CVSS 9.1 - The vulnerability in the SLC 500 controller platform occurs when the controller\uf\uf Status file property is not set to Static thereby allowing changes to the file contents.	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/511407
10.10.11.1	CVE-2010-5305: CVSS 9.8 - Password exposure by improper access control vulnerability	https://nvd.nist.gov/vuln/detail/CVE-2010-5305
10.10.11.1	RA-511407-2: CVSS 9.1 - The vulnerability in the SLC 500 controller platform occurs when the controller\uf\uf Status file property is not set to Static thereby allowing changes to the file contents.	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/511407

INSERT ASP LOGO HERE

Rockwell Automation

Spacely Sprockets – Mikwaukee, WI
VULNERABILITY DISCOVERY SERVICE

Asset	Description	Remediation Guidance
10.10.1.11	CVE-2010-5305: CVSS 9.8 - Password exposure by improper access control vulnerability	https://nvd.nist.gov/vuln/detail/CVE-2010-5305
10.10.1.11	RA-511407-2: CVSS 9.1 - The vulnerability in the SLC 500 controller platform occurs when the controller\uf\u Status file property is not set to Static thereby allowing changes to the file contents.	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/511407
10.10.2.63	CVE-2010-5305: CVSS 9.8 - Password exposure by improper access control vulnerability	https://nvd.nist.gov/vuln/detail/CVE-2010-5305
10.10.2.63	RA-511407-2: CVSS 9.1 - The vulnerability in the SLC 500 controller platform occurs when the controller\uf\u Status file property is not set to Static thereby allowing changes to the file contents.	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/511407
BOT107	CVE-2012-6437: CVSS 10.0 - Improper Authentication Vulnerability via Firmware Upload	https://nvd.nist.gov/vuln/detail/CVE-2012-6438
BOT107	CVE-2012-6440: CVSS 9.3 - Vulnerability could allow man-in-the-middle attackers to conduct replay attacks via HTTP traffic.	https://nvd.nist.gov/vuln/detail/CVE-2012-6440
BOT107	CVE-2012-6441: CVSS 10.0 - Vulnerability could allow Information Exposure	https://us-cert.cisa.gov/ics/advisories/ICSA-13-011-03
BOT107	CVE-2016-9343: CVSS 10.0 - Logix5000 Programmable Automation Controller Denial of Service/Buffer Overflow Vulnerability	https://nvd.nist.gov/vuln/detail/CVE-2016-9343
Labeller	RA-433320: CVSS 10.0 - ControlLogix 1756-EWEB Enhanced Web Server Firmware Upgrade Security Vulnerability	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/433320
BOT107	CVE-2021-22681: CVSS 9.8 - Claroty CVE - Private Key Extraction	https://nvd.nist.gov/vuln/detail/CVE-2021-22681
BOT107	RA-58964: CVSS 9.1 - Successful exploitation of this vulnerability could include Denial of Service (DoS)	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/58964
MM105	CVE-2012-6437: CVSS 10.0 - Improper Authentication Vulnerability via Firmware Upload	https://nvd.nist.gov/vuln/detail/CVE-2012-6438
MM105	CVE-2012-6440: CVSS 9.3 - Vulnerability could allow man-in-the-middle attackers to conduct replay attacks via HTTP traffic.	https://nvd.nist.gov/vuln/detail/CVE-2012-6440
MM105	CVE-2012-6441: CVSS 10.0 - Vulnerability could allow Information Exposure	https://us-cert.cisa.gov/ics/advisories/ICSA-13-011-03
MM105	CVE-2021-22681: CVSS 9.8 - Claroty CVE - Private Key Extraction	https://nvd.nist.gov/vuln/detail/CVE-2021-22681
MM105	RA-58964: CVSS 9.1 - Successful exploitation of this vulnerability could include Denial of Service (DoS)	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/58964

INSERT ASP LOGO HERE

Rockwell Automation

Spacely Sprockets – Mikwaukee, WI
VULNERABILITY DISCOVERY SERVICE

Asset	Description	Remediation Guidance
MM105	CVE-2010-2965: CVSS 10.0 - Modify arbitrary memory vulnerability in Wind River VxWorks 6	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2965
Labeller	CVE-2012-6437: CVSS 10.0 - Improper Authentication Vulnerability via Firmware Upload	https://nvd.nist.gov/vuln/detail/CVE-2012-6438
Labeller	CVE-2012-6440: CVSS 9.3 - Vulnerability could allow man-in-the-middle attackers to conduct replay attacks via HTTP traffic.	https://nvd.nist.gov/vuln/detail/CVE-2012-6440
Labeller	CVE-2012-6441: CVSS 10.0 - Vulnerability could allow Information Exposure	https://us-cert.cisa.gov/ics/advisories/ICSA-13-011-03
Labeller	CVE-2016-9343: CVSS 10.0 - Logix5000 Programmable Automation Controller Denial of Service/Buffer Overflow Vulnerability	https://nvd.nist.gov/vuln/detail/CVE-2016-9343
Labeller	CVE-2021-22681: CVSS 9.8 - Claroty CVE - Private Key Extraction	https://nvd.nist.gov/vuln/detail/CVE-2021-22681
Labeller	RA-433318: CVSS 9.1 - ControlLogix 1756-EWEB Enhanced Web Server FTP Server Security Vulnerability	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/433318
Labeller	CVE-2010-2965: CVSS 10.0 - Modify arbitrary memory vulnerability in Wind River VxWorks 6	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2965
SPS60	CVE-2012-6437: CVSS 10.0 - Improper Authentication Vulnerability via Firmware Upload	https://nvd.nist.gov/vuln/detail/CVE-2012-6438
SPS60	CVE-2012-6440: CVSS 9.3 - Vulnerability could allow man-in-the-middle attackers to conduct replay attacks via HTTP traffic.	https://nvd.nist.gov/vuln/detail/CVE-2012-6440
SPS60	CVE-2012-6441: CVSS 10.0 - Vulnerability could allow Information Exposure	https://us-cert.cisa.gov/ics/advisories/ICSA-13-011-03
SPS60	CVE-2021-22681: CVSS 9.8 - Claroty CVE - Private Key Extraction	https://nvd.nist.gov/vuln/detail/CVE-2021-22681
SPS60	RA-58964: CVSS 9.1 - Successful exploitation of this vulnerability could include Denial of Service (DoS)	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/58964
PLCFC_5	CVE-2012-6437: CVSS 10.0 - Improper Authentication Vulnerability via Firmware Upload	https://nvd.nist.gov/vuln/detail/CVE-2012-6438
PLCFC_5	CVE-2012-6440: CVSS 9.3 - Vulnerability could allow man-in-the-middle attackers to conduct replay attacks via HTTP traffic.	https://nvd.nist.gov/vuln/detail/CVE-2012-6440
PLCFC_5	CVE-2012-6441: CVSS 10.0 - Vulnerability could allow Information Exposure	https://us-cert.cisa.gov/ics/advisories/ICSA-13-011-03
PLCFC_5	CVE-2021-22681: CVSS 9.8 - Claroty CVE - Private Key Extraction	https://nvd.nist.gov/vuln/detail/CVE-2021-22681

INSERT ASP LOGO HERE

Rockwell Automation

Spacely Sprockets – Mikwaukee, WI
VULNERABILITY DISCOVERY SERVICE

Asset	Description	Remediation Guidance
PLCFC_5	RA-58964: CVSS 9.1 - Successful exploitation of this vulnerability could include Denial of Service (DoS)	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/58964
PLCFC_5	CVE-2010-2965: CVSS 10.0 - Modify arbitrary memory vulnerability in Wind River VxWorks 6	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2965
SD59	CVE-2010-2965: CVSS 10.0 - Modify arbitrary memory vulnerability in Wind River VxWorks 6	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2965
SD59	CVE-2012-6437: CVSS 10.0 - Improper Authentication Vulnerability via Firmware Upload	https://nvd.nist.gov/vuln/detail/CVE-2012-6438
SD59	CVE-2012-6440: CVSS 9.3 - Vulnerability could allow man-in-the-middle attackers to conduct replay attacks via HTTP traffic.	https://nvd.nist.gov/vuln/detail/CVE-2012-6440
SD59	CVE-2012-6441: CVSS 10.0 - Vulnerability could allow Information Exposure	https://us-cert.cisa.gov/ics/advisories/ICSA-13-011-03
SD59	CVE-2016-20009: CVSS 9.8 - DNS Name:Wreck Vulnerabilities Affect Multiple Rockwell Automation and ABB Products	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-20009
SD59	CVE-2016-9343: CVSS 10.0 - Logix5000 Programmable Automation Controller Denial of Service/Buffer Overflow Vulnerability	https://nvd.nist.gov/vuln/detail/CVE-2016-9343
SD59	CVE-2019-12255: CVSS 9.8 - (Urgent/11) TCP Urgent Pointer = 0 leads to integer underflow	https://search.abb.com/library/Download.aspx?DocumentID=7PAA000401&LanguageCode=en&Action=Launch
SD59	CVE-2019-12256: CVSS 9.8 - (Urgent/11) TCP Urgent Pointer = 0 leads to integer underflow	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12256
SD59	CVE-2019-12261: CVSS 9.8 - (Urgent/11) TCP Urgent Pointer state confusion during connect() to a remote host	https://search.abb.com/library/Download.aspx?DocumentID=7PAA000401&LanguageCode=en&Action=Launch
SD59	CVE-2019-12262: CVSS 9.8 - (Urgent/11) Handling of unsolicited Reverse Address Resolution Protocol (ARP) replies	https://search.abb.com/library/Download.aspx?DocumentID=7PAA000401&LanguageCode=en&Action=Launch
SD59	CVE-2021-22681: CVSS 9.8 - Claroty CVE - Private Key Extraction	https://nvd.nist.gov/vuln/detail/CVE-2021-22681
SPS75	CVE-2012-6437: CVSS 10.0 - Improper Authentication Vulnerability via Firmware Upload	https://nvd.nist.gov/vuln/detail/CVE-2012-6438
SPS75	CVE-2012-6440: CVSS 9.3 - Vulnerability could allow man-in-the-middle attackers to conduct replay attacks via HTTP traffic.	https://nvd.nist.gov/vuln/detail/CVE-2012-6440
SPS75	CVE-2012-6441: CVSS 10.0 - Vulnerability could allow Information Exposure	https://us-cert.cisa.gov/ics/advisories/ICSA-13-011-03
SPS75	CVE-2021-22681: CVSS 9.8 - Claroty CVE - Private Key Extraction	https://nvd.nist.gov/vuln/detail/CVE-2021-22681

INSERT ASP LOGO HERE

Rockwell Automation

Spacely Sprockets – Mikwaukee, WI
VULNERABILITY DISCOVERY SERVICE

Asset	Description	Remediation Guidance
SPS75	RA-58964: CVSS 9.1 - Successful exploitation of this vulnerability could include Denial of Service (DoS)	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/58964
SPS75	CVE-2010-2965: CVSS 10.0 - Modify arbitrary memory vulnerability in Wind River VxWorks 6	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2965
PLC_1	CVE-2012-6437: CVSS 10.0 - Improper Authentication Vulnerability via Firmware Upload	https://nvd.nist.gov/vuln/detail/CVE-2012-6438
PLC_1	CVE-2012-6440: CVSS 9.3 - Vulnerability could allow man-in-the-middle attackers to conduct replay attacks via HTTP traffic.	https://nvd.nist.gov/vuln/detail/CVE-2012-6440
PLC_1	CVE-2012-6441: CVSS 10.0 - Vulnerability could allow Information Exposure	https://us-cert.cisa.gov/ics/advisories/ICSA-13-011-03
PLC_1	CVE-2016-9343: CVSS 10.0 - Logix5000 Programmable Automation Controller Denial of Service/Buffer Overflow Vulnerability	https://nvd.nist.gov/vuln/detail/CVE-2016-9343
PLC_1	CVE-2021-22681: CVSS 9.8 - Claroty CVE - Private Key Extraction	https://nvd.nist.gov/vuln/detail/CVE-2021-22681
PLC_1	RA-58964: CVSS 9.1 - Successful exploitation of this vulnerability could include Denial of Service (DoS)	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/58964
Labeller	CVE-2012-6437: CVSS 10.0 - Improper Authentication Vulnerability via Firmware Upload	https://nvd.nist.gov/vuln/detail/CVE-2012-6438
Labeller	CVE-2012-6440: CVSS 9.3 - Vulnerability could allow man-in-the-middle attackers to conduct replay attacks via HTTP traffic.	https://nvd.nist.gov/vuln/detail/CVE-2012-6440
Labeller	CVE-2012-6441: CVSS 10.0 - Vulnerability could allow Information Exposure	https://us-cert.cisa.gov/ics/advisories/ICSA-13-011-03
Labeller	CVE-2016-9343: CVSS 10.0 - Logix5000 Programmable Automation Controller Denial of Service/Buffer Overflow Vulnerability	https://nvd.nist.gov/vuln/detail/CVE-2016-9343
Labeller	CVE-2021-22681: CVSS 9.8 - Claroty CVE - Private Key Extraction	https://nvd.nist.gov/vuln/detail/CVE-2021-22681
Labeller	RA-433318: CVSS 9.1 - ControlLogix 1756-EWEB Enhanced Web Server FTP Server Security Vulnerability	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/433318
Labeller	RA-433320: CVSS 10.0 - ControlLogix 1756-EWEB Enhanced Web Server Firmware Upgrade Security Vulnerability	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/433320
Labeller	RA-58964: CVSS 9.1 - Successful exploitation of this vulnerability could include Denial of Service (DoS)	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/58964
Labeller	CVE-2010-2965: CVSS 10.0 - Modify arbitrary memory vulnerability in Wind River VxWorks 6	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2965

INSERT ASP LOGO HERE

Rockwell Automation

Spacely Sprockets – Mikwaukee, WI
VULNERABILITY DISCOVERY SERVICE

Asset	Description	Remediation Guidance
Labeller5	CVE-2012-6441: CVSS 10.0 - Vulnerability could allow Information Exposure	https://us-cert.cisa.gov/ics/advisories/ICSA-13-011-03
Labeller5	CVE-2021-22681: CVSS 9.8 - Claroty CVE - Private Key Extraction	https://nvd.nist.gov/vuln/detail/CVE-2021-22681
Labeller5	RA-433318: CVSS 9.1 - ControlLogix 1756-EWEB Enhanced Web Server FTP Server Security Vulnerability	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/433318
Labeller5	RA-433320: CVSS 10.0 - ControlLogix 1756-EWEB Enhanced Web Server Firmware Upgrade Security Vulnerability	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/433320
Labeler2	CVE-2012-6441: CVSS 10.0 - Vulnerability could allow Information Exposure	https://us-cert.cisa.gov/ics/advisories/ICSA-13-011-03
Labeler2	CVE-2016-9343: CVSS 10.0 - Logix5000 Programmable Automation Controller Denial of Service/Buffer Overflow Vulnerability	https://nvd.nist.gov/vuln/detail/CVE-2016-9343
Labeler2	CVE-2021-22681: CVSS 9.8 - Claroty CVE - Private Key Extraction	https://nvd.nist.gov/vuln/detail/CVE-2021-22681
Labeler2	RA-433318: CVSS 9.1 - ControlLogix 1756-EWEB Enhanced Web Server FTP Server Security Vulnerability	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/433318
Labeler2	RA-433320: CVSS 10.0 - ControlLogix 1756-EWEB Enhanced Web Server Firmware Upgrade Security Vulnerability	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/433320
Labeler2	RA-58964: CVSS 9.1 - Successful exploitation of this vulnerability could include Denial of Service (DoS)	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/58964
PLC_5	CVE-2012-6441: CVSS 10.0 - Vulnerability could allow Information Exposure	https://us-cert.cisa.gov/ics/advisories/ICSA-13-011-03
PLC_5	CVE-2021-22681: CVSS 9.8 - Claroty CVE - Private Key Extraction	https://nvd.nist.gov/vuln/detail/CVE-2021-22681
PLC_5	RA-433318: CVSS 9.1 - ControlLogix 1756-EWEB Enhanced Web Server FTP Server Security Vulnerability	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/433318
PLC_5	RA-433320: CVSS 10.0 - ControlLogix 1756-EWEB Enhanced Web Server Firmware Upgrade Security Vulnerability	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/433320
10.10.5.3	CVE-2012-6437: CVSS 10.0 - Improper Authentication Vulnerability via Firmware Upload	https://nvd.nist.gov/vuln/detail/CVE-2012-6438
10.10.5.3	CVE-2012-6440: CVSS 9.3 - Vulnerability could allow man-in-the-middle attackers to conduct replay attacks via HTTP traffic.	https://nvd.nist.gov/vuln/detail/CVE-2012-6440
10.10.5.3	CVE-2012-6441: CVSS 10.0 - Vulnerability could allow Information Exposure	https://us-cert.cisa.gov/ics/advisories/ICSA-13-011-03

INSERT ASP LOGO HERE

Rockwell Automation

Spacely Sprockets – Mikwaukee, WI
VULNERABILITY DISCOVERY SERVICE

Asset	Description	Remediation Guidance
10.10.5.3	CVE-2015-6490: CVSS 9.8 - A Remote Code Execution condition may result when an affected product receives a specific malicious web request	https://www.us-cert.gov/ics/advisories/ICSA-15-300-03A
10.10.5.3	CVE-2016-0868: CVSS 9.8 - A Remote Code Execution (RCE) condition may result when an affected product receives a specific malicious web request	https://nvd.nist.gov/vuln/detail/CVE-2016-0868
10.10.5.85	CVE-2017-7902: CVSS 9.8 - Improper Nonce Usage	https://nvd.nist.gov/vuln/detail/CVE-2017-7902
10.10.5.3	CVE-2017-14462: CVSS 9.8 - Modification of Communication Protocols and Network Configuration	https://nvd.nist.gov/vuln/detail/CVE-2017-14462
10.10.5.3	CVE-2017-14463: CVSS 9.8 - Overwriting the PLC Ladder Logic	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14463
10.10.5.3	CVE-2017-14464: CVSS 9.8 - Memory Module mismatch Fault	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/1072942
10.10.5.3	CVE-2017-14465: CVSS 9.8 - Forcing PLC I/O	https://nvd.nist.gov/vuln/detail/CVE-2017-14465
10.10.5.3	CVE-2017-14466: CVSS 9.8 - Writing and Clearing Master Password (See **)	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14466
10.10.5.3	CVE-2017-14467: CVSS 9.8 - Perform online edits to ladder logic	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14467
10.10.5.3	CVE-2017-14468: CVSS 9.8 - Trigger the PLC to load program from Electrically Erasable Programmable Read-Only Memory (EEPROM)	https://nvd.nist.gov/vuln/detail/CVE-2017-14468
10.10.5.3	CVE-2017-14469: CVSS 9.8 - Setting an invalid value for the user fault routine	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14469
10.10.5.3	CVE-2017-14470: CVSS 9.8 - Setting float elements to invalid values	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14470
10.10.5.3	CVE-2017-14471: CVSS 9.8 - Setting fault bits in specific function files to cause a Denial of Service	https://nvd.nist.gov/vuln/detail/CVE-2017-14471
10.10.5.3	CVE-2017-14472: CVSS 9.8 - Reading Master Password (See **)	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14472
10.10.5.3	CVE-2017-14473: CVSS 9.8 - Reading Master Ladder Logic	https://nvd.nist.gov/vuln/detail/CVE-2017-14473
10.10.5.3	CVE-2017-7898: CVSS 9.8 - Weak Password Resolution	https://ics-cert.us-cert.gov/advisories/ICSA-17-115-04
10.10.5.3	CVE-2017-7899: CVSS 9.8 - User Credentials Sent via GET method	https://ics-cert.us-cert.gov/advisories/ICSA-17-115-04
10.10.5.3	CVE-2017-7902: CVSS 9.8 - Improper Nonce Usage	https://nvd.nist.gov/vuln/detail/CVE-2017-7902
10.10.5.3	CVE-2017-7903: CVSS 9.8 - Weak Password Resolution	https://www.us-cert.gov/ics/advisories/ICSA-17-115-04

INSERT ASP LOGO HERE

Rockwell Automation

Asset	Description	Remediation Guidance
10.10.5.3	CVE-2020-6984: CVSS 9.8 - The cryptographic function utilized to protect the password in MicroLogix is discoverable. This password protects access to the device. If successfully exploited a remote attacker could gain unauthorized access to the controller.	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1124849
10.10.5.3	CVE-2020-6990: CVSS 9.8 - Use of Hard-Coded Cryptographic Key	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1124849
10.10.5.85	CVE-2012-6437: CVSS 10.0 - Improper Authentication Vulnerability via Firmware Upload	https://nvd.nist.gov/vuln/detail/CVE-2012-6438
10.10.5.85	CVE-2012-6440: CVSS 9.3 - Vulnerability could allow man-in-the-middle attackers to conduct replay attacks via HTTP traffic.	https://nvd.nist.gov/vuln/detail/CVE-2012-6440
10.10.5.85	CVE-2012-6441: CVSS 10.0 - Vulnerability could allow Information Exposure	https://us-cert.cisa.gov/ics/advisories/ICSA-13-011-03
10.10.5.85	CVE-2015-6490: CVSS 9.8 - A Remote Code Execution condition may result when an affected product receives a specific malicious web request	https://www.us-cert.gov/ics/advisories/ICSA-15-300-03A
10.10.5.85	CVE-2017-14462: CVSS 9.8 - Modification of Communication Protocols and Network Configuration	https://nvd.nist.gov/vuln/detail/CVE-2017-14462
10.10.5.85	CVE-2017-14463: CVSS 9.8 - Overwriting the PLC Ladder Logic	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14463
10.10.5.85	CVE-2017-14464: CVSS 9.8 - Memory Module mismatch Fault	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/1072942
10.10.5.85	CVE-2017-14465: CVSS 9.8 - Forcing PLC I/O	https://nvd.nist.gov/vuln/detail/CVE-2017-14465
10.10.5.85	CVE-2017-14466: CVSS 9.8 - Writing and Clearing Master Password (See **)	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14466
10.10.5.85	CVE-2017-14467: CVSS 9.8 - Perform online edits to ladder logic	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14467
10.10.5.85	CVE-2017-14468: CVSS 9.8 - Trigger the PLC to load program from Electrically Erasable Programmable Read-Only Memory (EEPROM)	https://nvd.nist.gov/vuln/detail/CVE-2017-14468
10.10.5.85	CVE-2017-14469: CVSS 9.8 - Setting an invalid value for the user fault routine	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14469
10.10.5.85	CVE-2017-14470: CVSS 9.8 - Setting float elements to invalid values	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14470
10.10.5.85	CVE-2017-14471: CVSS 9.8 - Setting fault bits in specific function files to cause a Denial of Service	https://nvd.nist.gov/vuln/detail/CVE-2017-14471
10.10.5.85	CVE-2017-14472: CVSS 9.8 - Reading Master Password (See **)	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14472

Spacely Sprockets – Mikwaukee, WI
VULNERABILITY DISCOVERY SERVICE

Asset	Description	Remediation Guidance
10.10.5.85	CVE-2017-14473: CVSS 9.8 - Reading Master Ladder Logic	https://nvd.nist.gov/vuln/detail/CVE-2017-14473
10.10.5.85	CVE-2017-16740: CVSS 10.0 - Execute CodeOverflow vulnerability in Rockwell	https://nvd.nist.gov/vuln/detail/CVE-2017-16740
10.10.5.85	CVE-2017-7898: CVSS 9.8 - Weak Password Resolution	https://ics-cert.us-cert.gov/advisories/ICSA-17-115-04
10.10.5.85	CVE-2017-7899: CVSS 9.8 - User Credentials Sent via GET method	https://ics-cert.us-cert.gov/advisories/ICSA-17-115-04
10.10.5.85	CVE-2017-7903: CVSS 9.8 - Weak Password Resolution	https://www.us-cert.gov/ics/advisories/ICSA-17-115-04
10.10.5.85	CVE-2020-6984: CVSS 9.8 - The cryptographic function utilized to protect the password in MicroLogix is discoverable. This password protects access to the device. If successfully exploited a remote attacker could gain unauthorized access to the controller.	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1124849
10.10.5.85	CVE-2020-6990: CVSS 9.8 - Use of Hard-Coded Cryptographic Key	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1124849
AF31	CVE-2022-1161: CVSS 10.0 - Claroty CVE - Modification of PLC Program Code	https://nvd.nist.gov/vuln/detail/CVE-2022-1161
10.10.5.85	RA-278864: CVSS 10.0 - Security vulnerability in password mechanism of MicroLogix	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/278864
10.10.5.85	RA-511407-1: CVSS 9.1 - The vulnerability in the MicroLogix controller platform occurs due to inadequate write protection measures on the controller﹐ Status file.	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/511407
10987	CVE-2012-6437: CVSS 10.0 - Improper Authentication Vulnerability via Firmware Upload	https://nvd.nist.gov/vuln/detail/CVE-2012-6438
10987	CVE-2012-6440: CVSS 9.3 - Vulnerability could allow man-in-the-middle attackers to conduct replay attacks via HTTP traffic.	https://nvd.nist.gov/vuln/detail/CVE-2012-6440
10987	CVE-2012-6441: CVSS 10.0 - Vulnerability could allow Information Exposure	https://us-cert.cisa.gov/ics/advisories/ICSA-13-011-03
10987	CVE-2016-9343: CVSS 10.0 - Logix5000 Programmable Automation Controller Denial of Service/Buffer Overflow Vulnerability	https://nvd.nist.gov/vuln/detail/CVE-2016-9343
10987	CVE-2021-22681: CVSS 9.8 - Claroty CVE - Private Key Extraction	https://nvd.nist.gov/vuln/detail/CVE-2021-22681
10987	CVE-2022-1161: CVSS 10.0 - Claroty CVE - Modification of PLC Program Code	https://nvd.nist.gov/vuln/detail/CVE-2022-1161
CIP_39963	CVE-2012-6440: CVSS 9.3 - Vulnerability could allow man-in-the-middle attackers to conduct replay attacks via HTTP traffic.	https://nvd.nist.gov/vuln/detail/CVE-2012-6440

INSERT ASP LOGO HERE

Rockwell Automation

Spacely Sprockets – Mikwaukee, WI
VULNERABILITY DISCOVERY SERVICE

Asset	Description	Remediation Guidance
AF31	CVE-2012-6437: CVSS 10.0 - Improper Authentication Vulnerability via Firmware Upload	https://nvd.nist.gov/vuln/detail/CVE-2012-6438
AF31	CVE-2012-6440: CVSS 9.3 - Vulnerability could allow man-in-the-middle attackers to conduct replay attacks via HTTP traffic.	https://nvd.nist.gov/vuln/detail/CVE-2012-6440
AF31	CVE-2012-6441: CVSS 10.0 - Vulnerability could allow Information Exposure	https://us-cert.cisa.gov/ics/advisories/ICSA-13-011-03
AF31	CVE-2016-9343: CVSS 10.0 - Logix5000 Programmable Automation Controller Denial of Service/Buffer Overflow Vulnerability	https://nvd.nist.gov/vuln/detail/CVE-2016-9343
AF31	CVE-2021-22681: CVSS 9.8 - Claroty CVE - Private Key Extraction	https://nvd.nist.gov/vuln/detail/CVE-2021-22681
AF34	CVE-2012-6437: CVSS 10.0 - Improper Authentication Vulnerability via Firmware Upload	https://nvd.nist.gov/vuln/detail/CVE-2012-6438
AF34	CVE-2012-6440: CVSS 9.3 - Vulnerability could allow man-in-the-middle attackers to conduct replay attacks via HTTP traffic.	https://nvd.nist.gov/vuln/detail/CVE-2012-6440
AF34	CVE-2012-6441: CVSS 10.0 - Vulnerability could allow Information Exposure	https://us-cert.cisa.gov/ics/advisories/ICSA-13-011-03
CIP_39963	CVE-2012-6441: CVSS 10.0 - Vulnerability could allow Information Exposure	https://us-cert.cisa.gov/ics/advisories/ICSA-13-011-03
AF34	CVE-2016-9343: CVSS 10.0 - Logix5000 Programmable Automation Controller Denial of Service/Buffer Overflow Vulnerability	https://nvd.nist.gov/vuln/detail/CVE-2016-9343
AF34	CVE-2021-22681: CVSS 9.8 - Claroty CVE - Private Key Extraction	https://nvd.nist.gov/vuln/detail/CVE-2021-22681
AF34	CVE-2022-1161: CVSS 10.0 - Claroty CVE - Modification of PLC Program Code	https://nvd.nist.gov/vuln/detail/CVE-2022-1161
CIP_39963	CVE-2012-6437: CVSS 10.0 - Improper Authentication Vulnerability via Firmware Upload	https://nvd.nist.gov/vuln/detail/CVE-2012-6438
CIP_39963	CVE-2016-20009: CVSS 9.8 - DNS Name:Wreck Vulnerabilities Affect Multiple Rockwell Automation and ABB Products	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-20009
CIP_39963	CVE-2021-22681: CVSS 9.8 - Claroty CVE - Private Key Extraction	https://nvd.nist.gov/vuln/detail/CVE-2021-22681
CIP_39963	CVE-2022-1161: CVSS 10.0 - Claroty CVE - Modification of PLC Program Code	https://nvd.nist.gov/vuln/detail/CVE-2022-1161
FVM	CVE-2012-6437: CVSS 10.0 - Improper Authentication Vulnerability via Firmware Upload	https://nvd.nist.gov/vuln/detail/CVE-2012-6438

INSERT ASP LOGO HERE

Rockwell Automation

Spacely Sprockets – Mikwaukee, WI
VULNERABILITY DISCOVERY SERVICE

Asset	Description	Remediation Guidance
FVM	CVE-2012-6440: CVSS 9.3 - Vulnerability could allow man-in-the-middle attackers to conduct replay attacks via HTTP traffic.	https://nvd.nist.gov/vuln/detail/CVE-2012-6440
FVM	CVE-2012-6441: CVSS 10.0 - Vulnerability could allow Information Exposure	https://us-cert.cisa.gov/ics/advisories/ICSA-13-011-03
FVM	CVE-2016-20009: CVSS 9.8 - DNS Name:Wreck Vulnerabilities Affect Multiple Rockwell Automation and ABB Products	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-20009
FVM	CVE-2021-22681: CVSS 9.8 - Claroty CVE - Private Key Extraction	https://nvd.nist.gov/vuln/detail/CVE-2021-22681
FVM	CVE-2022-1161: CVSS 10.0 - Claroty CVE - Modification of PLC Program Code	https://nvd.nist.gov/vuln/detail/CVE-2022-1161
Palletizer	CVE-2012-6437: CVSS 10.0 - Improper Authentication Vulnerability via Firmware Upload	https://nvd.nist.gov/vuln/detail/CVE-2012-6438
Palletizer	CVE-2012-6440: CVSS 9.3 - Vulnerability could allow man-in-the-middle attackers to conduct replay attacks via HTTP traffic.	https://nvd.nist.gov/vuln/detail/CVE-2012-6440
Palletizer	CVE-2012-6441: CVSS 10.0 - Vulnerability could allow Information Exposure	https://us-cert.cisa.gov/ics/advisories/ICSA-13-011-03
Palletizer	CVE-2016-20009: CVSS 9.8 - DNS Name:Wreck Vulnerabilities Affect Multiple Rockwell Automation and ABB Products	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-20009
Palletizer	CVE-2021-22681: CVSS 9.8 - Claroty CVE - Private Key Extraction	https://nvd.nist.gov/vuln/detail/CVE-2021-22681
Palletizer	CVE-2022-1161: CVSS 10.0 - Claroty CVE - Modification of PLC Program Code	https://nvd.nist.gov/vuln/detail/CVE-2022-1161
LOGIX	CVE-2012-6437: CVSS 10.0 - Improper Authentication Vulnerability via Firmware Upload	https://nvd.nist.gov/vuln/detail/CVE-2012-6438
LOGIX	CVE-2012-6440: CVSS 9.3 - Vulnerability could allow man-in-the-middle attackers to conduct replay attacks via HTTP traffic.	https://nvd.nist.gov/vuln/detail/CVE-2012-6440
LOGIX	CVE-2012-6441: CVSS 10.0 - Vulnerability could allow Information Exposure	https://us-cert.cisa.gov/ics/advisories/ICSA-13-011-03
LOGIX	CVE-2016-20009: CVSS 9.8 - DNS Name:Wreck Vulnerabilities Affect Multiple Rockwell Automation and ABB Products	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-20009
LOGIX	CVE-2021-22681: CVSS 9.8 - Claroty CVE - Private Key Extraction	https://nvd.nist.gov/vuln/detail/CVE-2021-22681
LOGIX	CVE-2022-1161: CVSS 10.0 - Claroty CVE - Modification of PLC Program Code	https://nvd.nist.gov/vuln/detail/CVE-2022-1161

INSERT ASP LOGO HERE

Rockwell Automation

Spacely Sprockets – Mikwaukee, WI
VULNERABILITY DISCOVERY SERVICE

Asset	Description	Remediation Guidance
HTST1	CVE-2012-6437: CVSS 10.0 - Improper Authentication Vulnerability via Firmware Upload	https://nvd.nist.gov/vuln/detail/CVE-2012-6438
HTST1	CVE-2012-6440: CVSS 9.3 - Vulnerability could allow man-in-the-middle attackers to conduct replay attacks via HTTP traffic.	https://nvd.nist.gov/vuln/detail/CVE-2012-6440
HTST1	CVE-2016-9343: CVSS 10.0 - Logix5000 Programmable Automation Controller Denial of Service/Buffer Overflow Vulnerability	https://nvd.nist.gov/vuln/detail/CVE-2016-9343
HTST1	CVE-2019-12255: CVSS 9.8 - (Urgent/11) TCP Urgent Pointer = 0 leads to integer underflow	https://search.abb.com/library/Download.aspx?DocumentID=7PAA000401&LanguageCode=en&Action=Launch
HTST1	CVE-2019-12261: CVSS 9.8 - (Urgent/11) TCP Urgent Pointer state confusion during connect() to a remote host	https://search.abb.com/library/Download.aspx?DocumentID=7PAA000401&LanguageCode=en&Action=Launch
Case_10635	CVE-2016-9343: CVSS 10.0 - Logix5000 Programmable Automation Controller Denial of Service/Buffer Overflow Vulnerability	https://nvd.nist.gov/vuln/detail/CVE-2016-9343
HTST1	CVE-2019-12262: CVSS 9.8 - (Urgent/11) Handling of unsolicited Reverse Address Resolution Protocol (ARP) replies	https://search.abb.com/library/Download.aspx?DocumentID=7PAA000401&LanguageCode=en&Action=Launch
HTST1	CVE-2021-22681: CVSS 9.8 - Claroty CVE - Private Key Extraction	https://nvd.nist.gov/vuln/detail/CVE-2021-22681
HTST1	RA-433319: CVSS 9.1 - ControlLogix 1756-EN2T EtherNet/IP Bridge Firmware Upgrade Security Vulnerability	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/433319
Case_10635	CVE-2021-22681: CVSS 9.8 - Claroty CVE - Private Key Extraction	https://nvd.nist.gov/vuln/detail/CVE-2021-22681
Case_10635	RA-58964: CVSS 9.1 - Successful exploitation of this vulnerability could include Denial of Service (DoS)	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/58964
MSPS_38	CVE-2016-9343: CVSS 10.0 - Logix5000 Programmable Automation Controller Denial of Service/Buffer Overflow Vulnerability	https://nvd.nist.gov/vuln/detail/CVE-2016-9343
MSPS_38	CVE-2021-22681: CVSS 9.8 - Claroty CVE - Private Key Extraction	https://nvd.nist.gov/vuln/detail/CVE-2021-22681
MSPS_38	RA-58964: CVSS 9.1 - Successful exploitation of this vulnerability could include Denial of Service (DoS)	https://rockwellautomation.custhelp.com/app/answers/detail/a_id/58964
10.10.5.68	CVE-2020-11901: CVSS 9.0 - Ripple20 - An improper input validation issue in the DNS resolver component when handling a sent packet.	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2020-175-01
10.10.12.13	CVE-2020-25176: CVSS 9.8 - Code Execution due to Relative Path Traversal	https://www.us-cert.gov/ics/advisories/icsa-20-280-01
10.10.12.11	CVE-2020-25176: CVSS 9.8 - Code Execution due to Relative Path Traversal	https://www.us-cert.gov/ics/advisories/icsa-20-280-01

INSERT ASP LOGO HERE

Rockwell Automation

The following table provides information about end-of-life or unsupported Windows operating systems that were discovered through the active scanning process. There may be additional operating systems that are no longer supported that were unable to be identified.

Table 2:2 – Unsupported Windows Operating Systems

Asset	Description	Remediation Guidance
Maint_PC	This asset is running the Windows 7 Operating System which no longer receives Security Patches and Updates, making it an easily exploitable attack surface.	Risk for Operating Systems that no longer receive security patches can be reduced by either migrating/updating to a new system or adding external protections or isolation to minimize the attack vectors. Additional consulting is required to determine the appropriate solution.
AVB2	This asset is running the Windows XP Operating System which no longer receives Security Patches and Updates, making it an easily exploitable attack surface.	Risk for Operating Systems that no longer receive security patches can be reduced by either migrating/updating to a new system or adding external protections or isolation to minimize the attack vectors. Additional consulting is required to determine the appropriate solution.
Imager	This asset is running the Windows XP Operating System which no longer receives Security Patches and Updates, making it an easily exploitable attack surface.	Risk for Operating Systems that no longer receive security patches can be reduced by either migrating/updating to a new system or adding external protections or isolation to minimize the attack vectors. Additional consulting is required to determine the appropriate solution.
Production	This asset is running the Windows 7 Operating System which no longer receives Security Patches and Updates, making it an easily exploitable attack surface.	Risk for Operating Systems that no longer receive security patches can be reduced by either migrating/updating to a new system or adding external protections or isolation to minimize the attack vectors. Additional consulting is required to determine the appropriate solution.

INSERT ASP LOGO HERE

Rockwell Automation

3 DATA COLLECTION INFORMATION

The section provides information about the data that was collected during the onsite visit. This will include:

- Scope Qualification Information
- Collection Network Information

The table shown below, provides the Scope Qualification information that was filled out during the data collection process. This information is important as it provides context to the data as this represents the strategy for how the data was collected and the environment in which it was collected.

Table 3:1 - Scope Qualification Information

Item	Topic Area	Question	Answer(s)	Technical Comments
1	Plant Area / Equipment	Describe Equipment, Application, Driven Devices	Various OT Devices	
2	Network	Do you have network documentation/drawings that you can provide?	No	
3	Network	Can the workstations be leveraged to discover near by network assets? How Many?	Yes	If NO, then the deployment personnel will need to connect their own machine to each network subnet/VLAN in scope
4	Network	Approx. how many VLAN's/Subnets will be in scope?	1	
5	Service Expectations	What are you looking for as part of this asset and vulnerability discovery survey?		
6	Policy	Are there any policies for requiring approval to run collection tools from either your own infrastructure, or field service laptop? Are there approvals required for deployment engineers to connect to the networks in scope?	Yes	The .exe that is leveraged will need to be approved and transferred from a usb device to each workstation
7	Misc.	Who are the point of contacts that will be assiting in this project? - Network Engineers - Plant Managers	Plant Engineer & I.T. Personell	

INSERT ASP LOGO HERE

Rockwell Automation

Item	Topic Area	Question	Answer(s)	Technical Comments
		- Maintenace Employees		

The Collection Network table provides information about the subnet(s) scanned, its reach within an architecture due to either a flat network (single vlan/subnet) or functional zones (multiple vlans/subnets), and the device IP where the network scan originated for each vlan/subnet.

Table 3:2 - Collection Network Information

Item	Subnet	Flat Network	Workstation Availability	Workstation/Collection IP
VLAN/Subnet 1	10.0.0.1/24	Flat Network	yes	10.10.10.16

INSERT ASP LOGO HERE

Rockwell Automation

4 SUMMARY OF SURVEY FINDINGS

This section provides a summary or overview of all the findings. This will include:

- Summary of Insights
- Device Communication Statistics
- Asset Identification

Insights assist in planning the proactive enhancement of your ICS security posture, shedding light on mission critical assets and misconfigurations. Select information from this summary is provided in further sections.

Table 4:1 - Insights Summary

Name	Description	Assets
Unsecured Protocols	1 asset is using unsecured protocols	1
Talking with External IPs	1 asset was communicating with external IPs	1
End Of Life Assets	70 assets are considered End of Life (EoL)	70
Full Match CVEs	67 assets have unpatched vulnerabilities - Full Match	67
Program Match CVEs	1 asset has vulnerabilities in its installed programs	1
Multiple Interfaces	10 assets have multiple network interfaces	10
Open Ports	1 asset has open ports	1
Vendor Match CVEs	1 asset has unpatched vulnerabilities - Vendor Match	1
Windows CVEs	5 assets have unpatched vulnerabilities - Windows Match	5
USB devices connected to assets	USB devices were connected to 1 asset	1

INSERT ASP LOGO HERE

Rockwell Automation

4.1 Device Communication Statistics

Basic statistical analysis of the communication between devices regarding who and how devices are communicating.

Table 4:2 – Counters

Vendors	OT Assets	IT Assets	IoT Assets	Protocols
8	183	45	0	12

Table 4:3 - Asset Distribution by Type

Asset Type	Percentage
Endpoint	18.5%
OT	6.9%
Remote IO	25.9%
PLC	25.9%
Networking	0.4%
Gateway	4.7%
Printer	0.4%
HMI	14.7%
Robot	0.9%

Table 4:4 - Asset Vendors

Identified Vendor	Percentage
Rockwell Automation	69%
Baumer IVO & KG	1.3%
HMS Industrial Networks	0.4%
Hewlett Packard	0.9%

Identified Vendor	Percentage
Siemens	2.2%
Lantronix	4.7%
ProSoft	0.4%
Fanuc Robotics	0.9%

4.2 Asset Identification

The first step in any Security Improvement Plan. Understanding what you have.

4.2.1 Critical Findings Assets Summary

The following list shows the devices that were determined to be critical either based on their assigned criticality within the Claroty platform or because they are referenced in a Critical Finding. Devices are only discovered from scanned subnets. A complete list of all devices and device information is provided in the Comprehensive Data Report spreadsheet.

Table 4:5 - Connected Asset

Asset ID	Name	Mac	Firmware	OS	Type	Vendor	Protocols	Criticality
59	10.10.1.111:Card 1 \ 192.168.1.12	-	V3.007	-	Remote IO	Rockwell Automation	-	High
64	ECN31	-	V4.002	-	Remote IO	Rockwell Automation	-	High
66	IO93_86	-	V1.008	-	Remote IO	Rockwell Automation	-	High
67	IO92_84	-	V1.008	-	Remote IO	Rockwell Automation	-	High
68	COMS30_30	-	V4.002	-	Remote IO	Rockwell Automation	-	High
69	IO90_81	-	V1.009	-	Remote IO	Rockwell Automation	-	High
70	AF10_21	-	V3.001	-	Remote IO	Rockwell Automation	-	High

Spacely Sprockets – Mikwaukee, WI
VULNERABILITY DISCOVERY SERVICE

Asset ID	Name	Mac	Firmware	OS	Type	Vendor	Protocols	Criticality
71	IO94_88	-	V1.009	-	Remote IO	Rockwell Automation	-	High
72	COMS50_43	-	V4.002	-	Remote IO	Rockwell Automation	-	High
73	AF10_15	-	V5.001	-	Remote IO	Rockwell Automation	-	High
74	IO90_80	-	V1.008	-	Remote IO	Rockwell Automation	-	High
75	AF10_20	-	V3.001	-	Remote IO	Rockwell Automation	-	High
79	ECN31	-	V4.002	-	Remote IO	Rockwell Automation	-	High
81	IO93_86	-	V1.008	-	Remote IO	Rockwell Automation	-	High
82	IO92_84	-	V1.009	-	Remote IO	Rockwell Automation	-	High
83	COMS30_30	-	V4.002	-	Remote IO	Rockwell Automation	-	High
84	IO90_81	-	V1.008	-	Remote IO	Rockwell Automation	-	High
85	AF10_21	-	V2.001	-	Remote IO	Rockwell Automation	-	High
86	IO94_88	-	V1.009	-	Remote IO	Rockwell Automation	-	High
87	COMS50_43	-	V4.002	-	Remote IO	Rockwell Automation	-	High
88	AF10_15	-	V5.001	-	Remote IO	Rockwell Automation	-	High
89	IO90_80	-	V1.008	-	Remote IO	Rockwell Automation	-	High
90	AF10_20	-	V3.001	-	Remote IO	Rockwell Automation	-	High

INSERT ASP LOGO HERE

Rockwell Automation

Spacely Sprockets – Mikwaukee, WI
VULNERABILITY DISCOVERY SERVICE

Asset ID	Name	Mac	Firmware	OS	Type	Vendor	Protocols	Criticality
102	10.10.2.43:Card 6 \ 191.16.117.27	-	V4.001	-	Remote IO	Rockwell Automation	-	High
103	AF45	-	V5.012	-	Remote IO	Rockwell Automation	-	High
104	AF250	-	V5.012	-	Remote IO	Rockwell Automation	-	High
106	10.10.2.43:Card 6 \ 191.16.117.24	-	V4.001	-	Remote IO	Rockwell Automation	-	High
107	10.10.2.43:Card 6 \ 191.16.117.23	-	V4.001	-	Remote IO	Rockwell Automation	-	High
108	10.10.2.43:Card 6 \ 191.16.117.22	-	V4.001	-	Remote IO	Rockwell Automation	-	High
109	AF12	-	V5.012	-	Remote IO	Rockwell Automation	-	High
110	AF60	-	V5.012	-	Remote IO	Rockwell Automation	-	High
111	AF11	-	V5.012	-	Remote IO	Rockwell Automation	-	High
112	10.10.2.43:Card 6 \ 191.16.117.26	-	V7.001	-	Remote IO	Rockwell Automation	-	High
113	10.10.2.43:Card 6 \ 191.16.117.21	-	V4.001	-	Remote IO	Rockwell Automation	-	High
123	COMS50_43	-	V4.002	-	Remote IO	Rockwell Automation	-	High
124	ECN31	-	V4.002	-	Remote IO	Rockwell Automation	-	High
125	IO94_88	-	V1.009	-	Remote IO	Rockwell Automation	-	High
126	10.10.2.113:Card 3 \ 192.168.1.20	-	V2.001	-	Remote IO	Rockwell Automation	-	High
127	IO93_86	-	V1.009	-	Remote IO	Rockwell Automation	-	High

INSERT ASP LOGO HERE

Rockwell Automation

Spacely Sprockets – Mikwaukee, WI
VULNERABILITY DISCOVERY SERVICE

Asset ID	Name	Mac	Firmware	OS	Type	Vendor	Protocols	Criticality
128	IO90_80	-	V1.009	-	Remote IO	Rockwell Automation	-	High
129	10.10.2.113:Card 3 \ 192.168.1.21	-	V3.001	-	Remote IO	Rockwell Automation	-	High
130	10.10.2.113:Card 3 \ 192.168.1.15	-	V5.001	-	Remote IO	Rockwell Automation	-	High
131	IO90_81	-	V1.009	-	Remote IO	Rockwell Automation	-	High
132	COMS30_30	-	V4.002	-	Remote IO	Rockwell Automation	-	High
133	IO92_84	-	V1.009	-	Remote IO	Rockwell Automation	-	High
143	10.10.3.37:Card 2 \ 192.168.1.202	-	V5.001	-	Remote IO	Rockwell Automation	-	High
148	Flex_IO	-	V4.003	-	Remote IO	Rockwell Automation	-	High
152	10.10.3.37:Card 2 \ 192.168.1.201	-	V5.001	-	Remote IO	Rockwell Automation	-	High
190	E205	-	V4.003	-	PLC	Rockwell Automation	-	High
191	D406	-	V4.003	-	PLC	Rockwell Automation	-	High
192	S206	-	V4.003	-	PLC	Rockwell Automation	-	High
193	E200	-	V6.004	-	Remote IO	Rockwell Automation	-	High
194	Q520	-	V3.003	-	Remote IO	Rockwell Automation	-	High
195	J506	-	V4.003	-	PLC	Rockwell Automation	-	High
196	C206	-	V4.003	-	PLC	Rockwell Automation	-	High

INSERT ASP LOGO HERE

Rockwell Automation

Asset ID	Name	Mac	Firmware	OS	Type	Vendor	Protocols	Criticality
197	C700	-	V3.003	-	Remote IO	Rockwell Automation	-	High
204	CTF002	-	V5.001	-	Remote IO	Rockwell Automation	-	High
205	IO_1	-	V4.002	-	Remote IO	Rockwell Automation	-	High
206	CTF001	-	V5.001	-	Remote IO	Rockwell Automation	-	High
207	TC001	-	V7.002	-	Remote IO	Rockwell Automation	-	High
208	TCD_D	-	V6.001	-	Remote IO	Rockwell Automation	-	High
209	TC002	-	V6.002	-	Remote IO	Rockwell Automation	-	High
210	TC003	-	V6.002	-	Remote IO	Rockwell Automation	-	High
221	AF31	00:00:BC:65:E1:9F,00:00:BC:65:E2:7B	V4.001	-	PLC	Rockwell Automation	CIP	High
227	SPS60	00:1D:9C:CD:75:0B,00:1D:9C:CD:D3:4A	V6.004	-	PLC	Rockwell Automation	CIP	High
233	AF34	00:00:BC:CD:39:FD,00:00:BC:CD:B2:C7	V4.001	-	PLC	Rockwell Automation	CIP	High
240	SD59	00:00:BC:05:0E:DF,00:1D:9C:CF:41:71	V1.030	-	PLC	Rockwell Automation	CIP	High
247	PLC_1	00:00:BC:C7:ED:0B,00:00:BC:C7:ED:DD	V6.001	-	PLC	Rockwell Automation	CIP	High
255	CONT_02	00:0E:8C:99:86:83	V2.6.0	-	PLC	Siemens	TCP	High

INSERT ASP LOGO HERE

Rockwell Automation

Spacely Sprockets – Mikwaukee, WI
VULNERABILITY DISCOVERY SERVICE

Asset ID	Name	Mac	Firmware	OS	Type	Vendor	Protocols	Criticality
256	Maint_PC	E0:DB:55:B7:DC:16	-	Windows 7	OT	Siemens	SMB	Medium
257	CONT_09	00:1B:1B:0C:02:27	V3.2.7	-	PLC	Siemens	TCP	High
258	CONT_09	00:1B:1B:07:BE:38	V3.2.7	-	PLC	Siemens	TCP	High
259	CONT_12	00:1B:1B:3B:18:EE	V3.2.6	-	PLC	Siemens	TCP	High
260	10.10.1.73	00:20:4A:82:B4:63	-	-	Gateway	Lantronix	UDP	High
261	10.10.2.67	00:20:4A:BE:34:FC	-	-	Gateway	Lantronix	UDP	High
262	10.10.1.141	00:20:4A:DF:BA:74	-	-	Gateway	Lantronix	UDP	High
263	10.10.1.53	00:20:4A:D4:07:95	-	-	Gateway	Lantronix	UDP	High
264	10.10.3.19	00:20:4A:E3:A7:90	-	-	Gateway	Lantronix	UDP	High
265	10.10.4.11	00:20:4A:F6:D9:F9	-	-	Gateway	Lantronix	UDP	High
266	10.10.1.35	00:20:4A:74:0A:2B	-	-	Gateway	Lantronix	UDP	High
267	10.10.1.71	00:20:4A:74:09:F7	-	-	Gateway	Lantronix	UDP	High
268	10.10.2.53	00:20:4A:64:83:01	-	-	Gateway	Lantronix	UDP	High
269	10.10.4.37	00:20:4A:68:5B:A0	-	-	Gateway	Lantronix	UDP	High
270	10.10.3.71	00:20:4A:74:4A:9A	-	-	Gateway	Lantronix	UDP	High
272	PVP343	00:1D:9C:BB:43:BF	6.00.04.16	-	HMI	Rockwell Automation	CIP, UDP	High

INSERT ASP LOGO HERE

Rockwell Automation

Spacely Sprockets – Mikwaukee, WI
VULNERABILITY DISCOVERY SERVICE

Asset ID	Name	Mac	Firmware	OS	Type	Vendor	Protocols	Criticality
273	MainHMI	00:1D:9C:DA:7F:DA	9.00.17.241	-	HMI	Rockwell Automation	CIP, UDP	High
274	PVP82	00:1D:9C:CF:20:37	8.00.10.12	-	HMI	Rockwell Automation	CIP, UDP	High
275	10.10.1.11	00:00:BC:CC:50:37	V3.011	-	PLC	Rockwell Automation	CIP	High
276	10.10.1.21	E4:90:69:A1:1D:DA	V3.013	-	PLC	Rockwell Automation	CIP	High
278	10.10.1.25	00:00:BC:1E:13:84	V3.011	-	PLC	Rockwell Automation	CIP	High
280	10.10.1.33	E4:90:69:A4:7F:2E	V3.013	-	PLC	Rockwell Automation	CIP	High
281	10.10.1.40	00:00:BC:39:68:DA	4.00.05.60	-	HMI	Rockwell Automation	CIP	High
282	MM105	00:00:BC:C6:E7:FC	V4.008	-	PLC	Rockwell Automation	CIP	High
283	10.10.1.42	00:00:BC:5A:35:97	5.00.04.55	-	HMI	Rockwell Automation	CIP	High
284	SPS75	00:00:BC:C6:E7:F0	V4.008	-	PLC	Rockwell Automation	CIP	High
285	10.10.1.44	00:00:BC:39:7F:C5	4.00.07.60	-	HMI	Rockwell Automation	CIP	High
287	10.10.1.61	E4:90:69:9C:FD:77	V3.013	-	PLC	Rockwell Automation	CIP	High
289	10.10.1.63	E4:90:69:A2:40:41	V3.013	-	PLC	Rockwell Automation	CIP	High
290	10.10.1.65	F4:54:33:A7:CA:4B	V3.013	-	PLC	Rockwell Automation	CIP	High
292	10.10.1.112	00:00:BC:C8:5D:83	5.10.06.09	-	HMI	Rockwell Automation	CIP	High
293	Labeller	00:00:BC:22:E3:08,00:00:BC:C7:F3:	V6.001	-	PLC	Rockwell Automation	CIP	High

INSERT ASP LOGO HERE

Rockwell Automation

Asset ID	Name	Mac	Firmware	OS	Type	Vendor	Protocols	Criticality
		A3,00:00:BC:C7:F3:FA						
294	Labeller	00:00:BC:22:E3:A2,00:00:BC:C7:EB:9B,00:00:BC:C8:21:A7	V6.001	-	PLC	Rockwell Automation	CIP	High
295	10.10.1.122	00:00:BC:C8:61:58	5.10.06.09	-	HMI	Rockwell Automation	CIP	High
297	10.10.2.11	00:00:BC:CC:C7:EA	V3.011	-	PLC	Rockwell Automation	CIP	High
299	10.10.2.21	00:00:BC:1E:0A:1C	V3.006	-	PLC	Rockwell Automation	CIP	High
302	10.10.2.25	00:00:BC:37:0C:B4	V3.011	-	PLC	Rockwell Automation	CIP	High
303	10.10.2.31	00:00:BC:61:9F:D5	V3.011	-	PLC	Rockwell Automation	CIP	High
305	10.10.2.61	00:00:BC:1E:31:AE	V3.006	-	PLC	Rockwell Automation	CIP	High
306	10.10.2.63	E4:90:69:9C:AF:23	V3.013	-	PLC	Rockwell Automation	CIP	High
307	Labeler2	00:00:BC:D1:23:DB,00:00:BC:D1:28:FB,00:00:BC:D1:B5:84	V6.005	-	PLC	Rockwell Automation	CIP	High
308	10.10.3.1	00:00:BC:1E:A9:02	V3.010	-	PLC	Rockwell Automation	CIP	High
310	10.10.3.11	00:00:BC:37:98:48	V3.011	-	PLC	Rockwell Automation	CIP	High
311	10.10.3.23	E4:90:69:A2:4A:FD	V3.013	-	PLC	Rockwell Automation	CIP	High
313	10.10.3.31	E4:90:69:AA:12:03	V3.013	-	PLC	Rockwell Automation	CIP	High
314	10.10.3.61	00:00:BC:64:1F:B0	V3.013	-	PLC	Rockwell Automation	CIP	High

INSERT ASP LOGO HERE

Rockwell Automation

Spacely Sprockets – Mikwaukee, WI
VULNERABILITY DISCOVERY SERVICE

Asset ID	Name	Mac	Firmware	OS	Type	Vendor	Protocols	Criticality
316	10.10.3.65	00:00:BC:63:6B:2A	V3.011	-	PLC	Rockwell Automation	CIP	High
317	10.10.5.3	00:1D:9C:A0:D0:B7	V2.014	-	PLC	Rockwell Automation	CIP	High
318	BOT107	00:1D:9C:CA:89:2B	V6.004	-	PLC	Rockwell Automation	CIP	High
319	10.10.5.12	00:00:BC:35:0C:D0	5.00.05.55	-	HMI	Rockwell Automation	CIP	High
320	Labeller5	00:00:BC:22:BE:32	V4.003	-	PLC	Rockwell Automation	CIP	High
321	PLC_5	00:00:BC:22:BE:45	V4.003	-	PLC	Rockwell Automation	CIP	High
322	10.10.5.25	E4:90:69:A2:86:A6	V3.013	-	PLC	Rockwell Automation	CIP	High
323	MSPS_38	00:00:BC:3D:99:3C	V6.006	-	PLC	Rockwell Automation	CIP	High
324	10.10.5.42	00:00:BC:B0:AF:6F	4.00.11.60	-	HMI	Rockwell Automation	CIP	High
325	Case_10635	00:00:BC:3E:24:30	V6.006	-	PLC	Rockwell Automation	CIP	High
326	Palletizer	00:00:BC:40:90:16	V19.015	-	PLC	Rockwell Automation	CIP	High
327	10.10.5.66	00:00:BC:3E:2E:CB	5.00.00.55	-	HMI	Rockwell Automation	CIP	High
328	10.10.5.68	F4:54:33:A4:A8:5D	V5.015	-	Remote IO	Rockwell Automation	CIP	High
329	LOGIX	00:00:BC:3E:0C:63	V16.003	-	PLC	Rockwell Automation	CIP	High
330	10.10.5.72	00:00:BC:30:16:50	5.00.04.55	-	HMI	Rockwell Automation	CIP	High
331	FVM	00:00:BC:40:2C:7B	V16.021	-	PLC	Rockwell Automation	CIP	High

INSERT ASP LOGO HERE

Rockwell Automation

Spacely Sprockets – Mikwaukee, WI
VULNERABILITY DISCOVERY SERVICE

Asset ID	Name	Mac	Firmware	OS	Type	Vendor	Protocols	Criticality
332	10.10.5.84	00:00:BC:B4:9E:E2	5.00.00.55	-	HMI	Rockwell Automation	CIP	High
333	10.10.5.85	00:00:BC:67:88:D7	V2.010	-	PLC	Rockwell Automation	CIP	High
334	CIP_39963	00:00:BC:40:2D:A7	V15.004	-	PLC	Rockwell Automation	CIP	High
335	PLCFC_5	00:00:BC:3E:75:BB	V3.009	-	PLC	Rockwell Automation	CIP	High
336	10.10.5.105	F4:54:33:A7:07:2A	V5.015	-	Remote IO	Rockwell Automation	CIP	High
337	10.10.10.1	00:00:BC:64:BF:79	V3.011	-	PLC	Rockwell Automation	CIP	High
339	10.10.11.1	E4:90:69:A6:52:D1	V3.013	-	PLC	Rockwell Automation	CIP	High
340	10.10.11.3	00:00:BC:CF:A7:07	V3.011	-	PLC	Rockwell Automation	CIP	High
341	10.10.11.5	00:00:BC:66:BC:F3	V3.011	-	PLC	Rockwell Automation	CIP	High
342	HTST1	00:00:BC:C9:2D:5D	V4.003	-	PLC	Rockwell Automation	CIP	High
343	10.10.12.1	00:00:BC:37:85:7F	V3.011	-	PLC	Rockwell Automation	CIP	High
344	10987	00:00:BC:25:43:7D	V1.003	-	PLC	Rockwell Automation	CIP	High
345	10.10.12.11	F4:54:33:AE:2F:77	V11.011	-	PLC	Rockwell Automation	CIP	High
347	10.10.12.13	F4:54:33:AF:77:45	V11.011	-	PLC	Rockwell Automation	CIP	High
349	10.10.13.4	00:00:BC:C8:1F:9C	5.10.06.09	-	HMI	Rockwell Automation	CIP	High
351	PVP187	00:1D:9C:CD:4E:13	8.00.10.12	-	HMI	Rockwell Automation	CIP, UDP	High

INSERT ASP LOGO HERE

Rockwell Automation

Spacely Sprockets – Mikwaukee, WI
VULNERABILITY DISCOVERY SERVICE

Asset ID	Name	Mac	Firmware	OS	Type	Vendor	Protocols	Criticality
356	10.10.1.46	00:00:BC:5E:B0:DF	5.10.00.09	-	HMI	Rockwell Automation	CIP	High
361	AVB2	00:14:D1:91:3A:71	-	Windows XP	Endpoint	-	SMB	Low
369	Imager	00:14:D1:92:15:31	-	Windows XP	Endpoint	-	SMB	Low
380	10.10.5.62	00:1D:9C:BA:AD:FC	5.10.11.09	-	HMI	Rockwell Automation	CIP	High
381	10.10.5.67	00:E0:E4:0A:25:F5	V2.002	-	Robot	Fanuc Robotics	UDP	High
382	10.10.5.69	00:E0:E4:0A:3C:22	V2.002	-	Robot	Fanuc Robotics	UDP	High
383	10.10.5.96	00:00:BC:3E:9A:B9	5.00.00.55	-	HMI	Rockwell Automation	CIP	High
384	10.10.5.98	00:00:BC:39:7F:BD	5.10.00.09	-	HMI	Rockwell Automation	CIP	High
395	Production	2C:27:D7:2B:0C:14	-	Windows 7	Endpoint	-	SMB	Low

END OF DELIVERABLE

INSERT ASP LOGO HERE

Rockwell Automation

INSERT ASP LOGO HERE

Rockwell Automation