Payatu

Company Name

Date

ICS Security Assessment Report

Client Details

Company Name: {{ Company Name }}

Contact Person: {{ Company Person of Contact }}

Email: poc@company.com

Telephone: +91 XXXXXXXXX

Document History

Version	Date	Author	Remark
1.0	{{ Date }}	Payatu Consultant	Initial Release

Contents

1. About Payatu..4

2. Project Details 5

2.1 Executive Summary 5
2.2 Scope and Objective..7
2.3 Project Timeline 8
2.4 ICS Assessment Workflow 8
2.5 Detailed Findings 10
2.5.1 Corporate Network Domain is Extended into Process Control Network 10
2.5.2 Unsupported Operating System and Applications 11
2.5.3 Inadequate ICS Network Boundary Protection 13
2.5.4 Inadequate Patch Management..15
2.5.5 Inadequate Configuration Management...16
2.5.6 Outdated Antivirus Definitions 17
2.6 Passive Scanning..19
2.6.1 CVE Details..19

3. Appendix...21

3.1 Evidence Screenshots 21
3.1.1 Unsupported Operating System and Applications 21
3.1.2 Inadequate Patch Management..24
3.1.3 Inadequate Configuration Management...25
3.1.4 Outdated Antivirus Definitions 26
3.2 Client's ICS Guidelines and Standards 27
3.3 OT Assessment Approach followed 27
3.3.1 Maturity Review, Risk Based Approach, Passive Scanning & Config Reviews...........27
3.3.2 Network Architecture Assessment..28
3.3.3 Network Layer Zone descriptions:..28

1. About Payatu

Payatu is a research-focused security testing service organization specialized in IoT and embedded products, web, mobile, cloud and infrastructure security assessments and in-depth technical security training. Our state-of-the-art research, methodologies, and tools ensure the safety of our client's assets.

At Payatu, we believe in following one's passion, and with that thought, we have created a world-class team of researchers and executors who are bending the rules to provide the best security services. We are a passionate bunch of folks working on the latest and leading-edge security technology.

We are proud to be part of a vibrant security community and don't miss any opportunity to give back. Some of the contributions in the following fields reflect our dedication and passion

nullcon - nullcon security conference is an annual security event held in Goa, India. After years of efforts put in the event, it has now become a world-renowned platform to showcase the latest and undisclosed research.
hardwear.io - Hardware security conference is an annual hardware security event held in The Hague, Netherlands. It is being organized to answer emerging threats and attacks on hardware. We aim to make it the largest platform where hardware security innovation happens.
Dedicated fuzzing infrastructure - We are proud to be one of the few security research companies to own an in-house infrastructure and hardware for distributed fuzzing of software such as browsers, client and server applications.
null - It all started with null - The open security community. It's a registered non-profit society and one of the most active security community. null is driven totally by passionate volunteers.
Open source - Our team regularly authors open source tools to aid in security learning and research.
Talks and Training: Our team delivers talks/highly technical training in various international security and hacking conference, i.e., DEFCON Las Vegas, BlackHat Las Vegas, HITB Amsterdam, Consecwest Vancouver, nullcon Goa, HackinParis Paris, Brucon Belgium, zer0con Seoul, PoC Seoul to name few.

We are catering to a diverse portfolio of clients across the world, who are leaders in banking, finance, technology, healthcare, manufacturing, media houses, information security, and education, including government agencies. Having various empanelment and accreditations, along with a strong word of mouth has helped us win new customers, and our thorough professionalism and quality of work, have brought repeat business from our existing clients.

We thank you for considering our security services and requesting a proposal. We look forward to extending the expertise of our passionate, world-class professionals to achieve your security objectives.

2. Project Details

2.1 Executive Summary

We performed a detailed assessment at the ICS SITE 1, ICS SITE 2 for the in-scope ICS infrastructure. During the activity, **we identified Seven (X) vulnerabilities; Four (Y) high, Three (Z) medium severity vulnerabilities**, which can allow a cyber-adversary to gain access to various ICS infrastructure.

Summary of ICS Assessment (Maturity Model)

We identified missing essential controls related to each capability. Below is the summary of the required controls to be built to enhance the cybersecurity posture of Client's OT assets:

Identify - Asset Management

- ICS Physical devices and software platforms within the organization are not inventoried.
- ...
- ...

Protect - Protective Technology

- No control is in place to enforce policy around removable media usage.
- ...
- ...

Protect - Access Control

- Access roles and access levels to various facilities assets are not clearly defined.
- ...
- ...

Protect - Awareness and Training

- There is no periodic security training for OT employees.
- ...
- ...

Detect - Security Continuous Monitoring

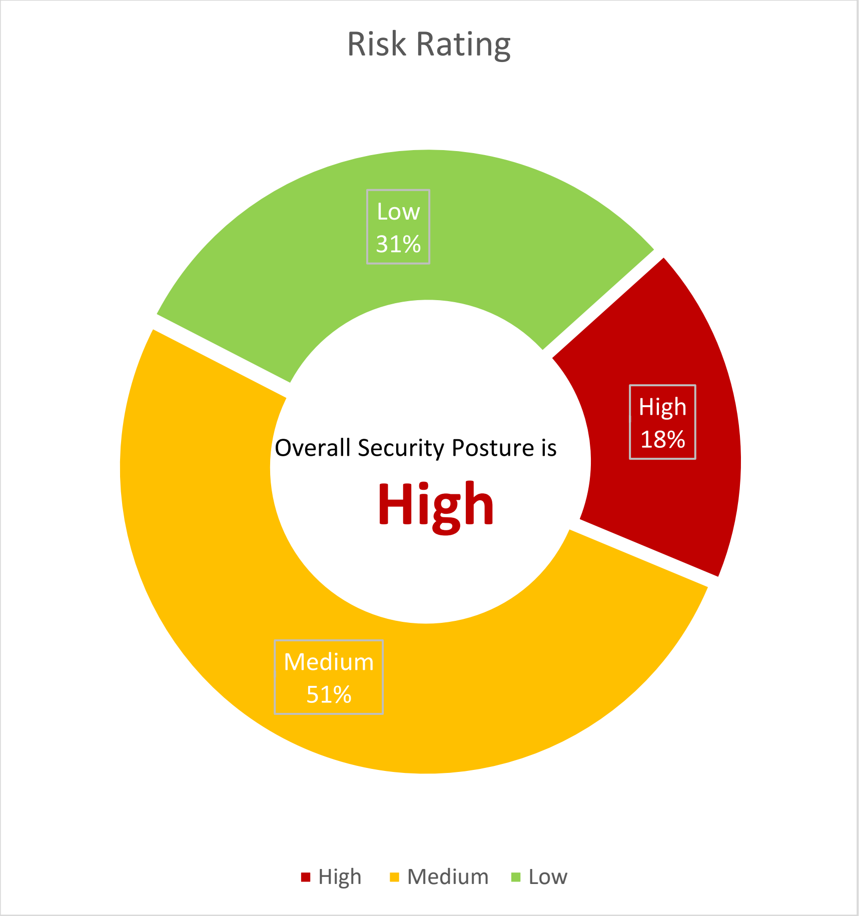
- No formal procedures or mechanisms established to monitor security events.
- ...
- ...
- ...

Detect - Anomalies and Events

- No Security Information and Event Management (SIEM) solution adopted in the OT assets. Hence, there is no aggregation and correlation of event data.
- …
- …

Summary of ICS Assessment (Risk Based Model)

We identified **N (N) security risks; X (X) high**, **Y (Y) medium and Z (Z) low** severity risks as part of the ICS security assessment. A summary of the identified security risks is outlined below:



Summary of Recommendations

Client should consider following corrective actions in order to address the issue criticality and reduce the ICS attack surface:

- **Maintain a full asset register** for all ICS sites through a defined process, using Asset Management Software and review and update on a defined frequency.
- Maintain a **physical and logical network architecture diagram** for all ICS sites.
- **Network Security/SIEM solutions** should be integrated within the control network to detect anomalies around Intrusions and for traffic inspection on a real-time basis.

- Gradually start **decommissioning the outdated insecure operating systems** and uninstall all unwanted software programs in order to reduce the attack surface in the future.
- …
- …
- …
- …

2.2 Scope and Objective

The ICS Security Assessment activity was carried out by the Payatu Team to identify the current cybersecurity risks of ICS Infrastructure and to provide adequate recommendations to mitigate any identified weaknesses. The overall activity including Fieldwork, Reporting, and Quality check reviews were carried out between <Date…> and <Date…>

Objective and Scope

The objective of conducting ICS Security Assessment activity is to provide Client with a detailed security assessment for ICS Infrastructure in place at Site's in order to strengthen the security and resilience of control systems throughout ICS Sites. Sample systems from DCS, ESD and F&G which are supporting the Site's processes were taken as part of the scope. The following table describes the scope of work:

ICS Site 1		
IP Address	**Hostname**	**Description**
		ESD Engg. Workstation
		FGS Engg. Workstation
		DCS Engg. Workstation
		OPC Server
		Domain Controller
		DCS Server
		DCS Server
		MIS Server
		MIS Server
		OPC Server
		Partial Stroke Test Server
		Alarm Server
		FGS & ESD workstation
		AMS Workstation

Testing Time Period

2.3 Project Timeline

The security assessment was performed for {{ count }} days from {{ start date }} to {{ end date }}.

2.4 ICS Assessment Workflow

The objective is to identify security weaknesses in the ICS infrastructure and subsequently provide recommendations to remediate these weaknesses. In order to achieve this objective, the Payatu Team followed a well-defined approach that's aligned to ISA/IEC 62443, NIST SP 800-82.

The assessment was divided into main 3 phases

Planning
Assessment
Reporting

Planning Phase: During this phase, an overview of the ICS Security Assessment was provided to stakeholders. Stakeholders were informed about the various activities that were to be performed during the assessment and made aware of the risk and impact of the assessment. The below highlighted activities were performed as part of this phase:

- Present the planned activities to the stakeholders.
- Define the detailed scope.
- Business understanding for control systems and DCS.
- Field visit for system interconnectivity understanding.
- Control network understanding.

Assessment Phase: During this phase, assessment and field testing activities were initiated. A discussion was carried out with stakeholders, field engineers and vendors to understand the field processes and assess the underlying systems supporting field operations.

- **Network enumeration** was performed to identify assets using netdiscover tool and verify connectivity between the test system and ICS network (Optional)
- **Work program** based interview was conducted with Vendors (e.g. Honeywell, Emerson) related to HMI applications and systems.
- **Network traffic capture** of DCS network using SPAN port was performed.

- **Automated vulnerability scan** of in scope ICS assets was performed along with a manual walkthrough of the Work Program. The review is performed in passive mode.
- **Network site reachability test** was conducted between ICS site and client's Corporate Network, ICS DMZ.

Activities	Outcome	Tools
Work program based interview	• Maturity Review • Risk Based Review	• CSET
Network enumeration	• IP addresses, Hostname • System Patches information • Vulnerable Softwares • Exposed and misconfigured services	• Manual Approach • Netdiscover • Windows Audit Scripts
Network traffic capture	• Network traffic packet capture files for malicious traffic analysis. • Network connectivity ports, Protocols usage in sites	• Wireshark • NetworkMiner • Passive scanning tools

Reporting Phase: In this phase, we drafted findings into a report that covers the effectiveness of technical controls, observed weaknesses and recommendations for enhancing cybersecurity resilience within ICS Sites. Below mentioned activities were performed:

- Analysis and reporting of findings related to ICS assets and HMIs discovered during the fieldwork testing activities.
- Analysis and reporting of findings related to operating systems vulnerabilities discovered during the fieldwork testing activities.
- Analysis and reporting of findings related to network traffic data capture discovered during the fieldwork testing activities.
- Analysis of reporting of findings related to general security controls.

NOTE: Please refer to appendix for a more info on methodology

Acronyms

The following table depicts the acronyms used in the report.

ICS	Industrial Control System
DCS	Distributed Control System
ESD	Emergency Shut Down
F&G	Fire and Gas
HMI	Human Machine Interface

SCADA	Supervisory Control and Data Acquisition
PLC	Programmable Logic Controller
RTU	Remote Terminal Unit

2.5 Detailed Findings

2.5.1 Corporate Network Domain is Extended into Process Control Network

Finding

We discovered assets in the process control network loaded with dual-homed network. Dual-homed computers can pass network traffic from one network to another allow extending access from the corporate domain to the assets on the field, result in bypassing several network based controls.

In a typical process control network, several hosts on the corporate network may configured to be dual-homed to permit access into the process control network. Historian servers often fall under this category, due to the need to use process data for performance monitoring and improvement purposes on the corporate network. The details of dual-homed assets are mentioned below:

Hostname	IP Address(es)	MAC Addresses	OS
RTYUIOP2	10.x.y.z, 192.168.y.z	00:0a:f7:f4:2a:11, 00:0a:f7:f4:2a:13	Server 2012 R2
RTYUIOP3	10.x.y.z, 192.168.y.z	c8:1f:66:cd:9f:e1, 00:0a:f7:7b:dd:98	Server 2012 R2

Criticality Rating

Criticality	Ease of Exploitability	Consequences
High	**Likely**	**Major**

Affected System / Devices / URL / Parameter

ICS Site		
• RTYUIOP2	• RTYUIOP6	• RTYUIOP2DAQ1
• RTYUIOP3	• RTYUIOP7	• RTYUIOP2DAQ8

Implication

Gaining access to these hosts can provide direct access into the process control network without having to use official remote access procedures. Even if historians are not provided extensive access into the process control network, observing their active network connections can reveal target IP address ranges. As a result of compromising the corporate network, it is a relatively simple task to locate users of interest on the corporate network and extract their passwords from memory. Adversary can make severe impact on the operation, health and safety from the corporate network.

Recommendation

To eliminate the security risk raised from dual-homed computers, Client should implement the following:

- Enforce security boundaries between control and corporate network by inspecting and filtering all connections between control network and corporate network using a network filtering firewall.
- ...

Management Response

Response/Action	Person Responsible	Proposed Completion Date

2.5.2 Unsupported Operating System and Applications

Finding

It was observed that the hosts are affected with multiple vulnerabilities due to the use of an obsolete /unsupported version of the operating system and applications. Microsoft will end support for Windows Server XXXX operating system by XXX XX, 2021. After this date, this product will no longer receive security patches that help protect systems from harmful viruses, spyware, and other malicious software.malware.

Criticality Rating

Criticality	Ease of Exploitability	Consequences
High	**Possible**	**Major**

Affected System / Devices / URL / Parameter

ICS SITE 1	ICS SITE 2
• A45DCSBMD101 • A6767DCSNSW01	• A19AMS71001 • B29OWS81001 • C29ESV9S1001

Implication

It was identified that unsupported or outdated operating systems along with the vulnerable version of applications are utilized in ICS operations. An attacker can leverage outdated operating systems or vulnerable applications to exploit the vulnerabilities and gain privileged access on the target systems which are used for managing and monitoring site operations (i.e. HMI Applications, Control systems). An attacker can utilize the compromised systems for focussed attacks or production disruption.

It was identified that the following outdated applications were installed on ICS Site's hosts:

- Microsoft Adobe Flash 17.x
- Microsoft Adobe Reader 10.x
- Microsoft Office 2007 - support ended on October 10, 2017
- Dell OpenManage System Management Software 8.2.x
- Microsoft SQL Server 2012
- Honeywell Experion station 431.3

Recommendation

- Client should define an asset management process in place and restrict deploying obsolete operating systems and applications.
- …
- …

In case of exception to perform Operating System Update to New Version :

If Operating system update is not possible due to business, software or contractual dependencies then,

- Client should ensure the systems is properly isolated in a network segment with restrict access from other network segment based on business requirements.
- …

Evidences

- Please refer to Appendix

Management Response

Response/Action	Person Responsible	Proposed Completion Date

2.5.3 Inadequate ICS Network Boundary Protection

Finding

It was observed that the systems supporting site operations (Production Monitoring using HMI, Logic controllers for Pressure value of valves and others) are not segregated in different network zones. Control systems related to DCS, ESD and F&G are assigned IP addresses in the same network range.

Criticality Rating

Criticality	Ease of Exploitability	Consequences
High	**Likely**	**Major**

Affected System / Devices / URL / Parameter

ICS SITE 1, ICS SITE 2
• ICS Network

Implication

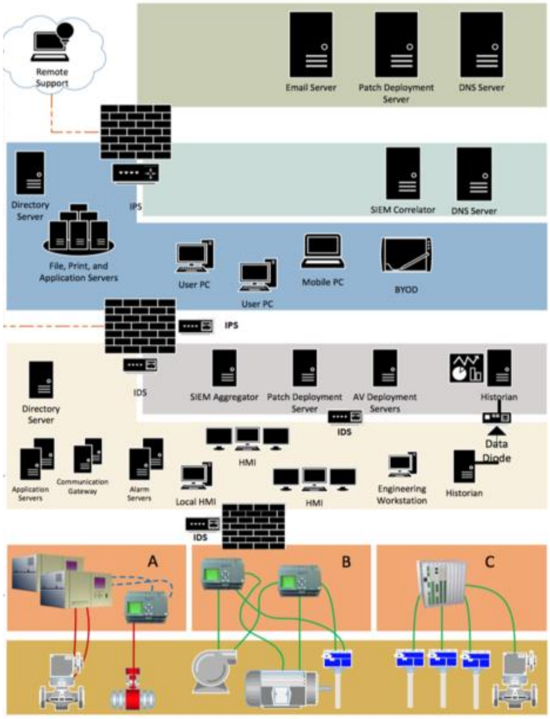
Weak boundary protection exposes ICS systems to elevated risks as a result of interfacing with devices and systems that directly support the control process. Any malware ransomware spread would not be contained in a segregated zone and will infect the entire control system network. Inadequate 'ICS Network' boundary protections for the ICS network make it more difficult to detect unauthorized activity.

Recommendation

- ICS Operations critical system, safety systems should be always placed in segregated network zones.
- Security intrusion detection and monitoring solutions should be in place to identify any existing or new threats within ICS network.

Additional Recommendations:

- As an additional layer of protection, security devices and systems need to be on a segregated network including AV, WSUS and Log servers which are used to support ICS system network equipment patching and updates (antivirus update server, Windows Server Update Services (WSUS) patch update, etc.).
- An ICS DMZ should be in place which houses a dedicated "jump" server based on approved business requirements only. Jump Server should permit only a limited and well-defined list of systems on the enterprise network (or those accessing via a remote method such as VPN) to access data elements derived from the ICS.
    - The Jump server should be hardened to run only essential services. Credentials for the jump server should not be the same as those used for authentication to systems on the enterprise network.
    - Restrict communication flows to the Jump server to a minimal subset of those required to support secure methods for accessing ICS systems (when needed to access from outside the standard ICS network).
    - Incorporate logging and monitoring of information derived from this system with continued verification



Purdue Model – ICS Secure Architecture

Evidences

- Please refer to Appendix.

Management Response

Response/Action	Person Responsible	Proposed Completion Date

2.5.4 Inadequate Patch Management

Finding

It was observed that security patches are not applied on a regular basis on the systems supporting ICS operations.

Criticality Rating

Criticality	Ease of Exploitability	Consequences
High	**Possible**	**Major**

Affected System / Devices / URL / Parameter

ICS SITE 1	ICS SITE 2
• M89DCSLOK101 • N67DCSNES101	• Q19MSA71001 • Y29OWD81001 • F29ESDDV9001

Implication

Control systems used for ICS operations with missing security patches could allow malicious agents to exploit vulnerabilities that exist on the ICS system, and may result in operational disruptions. Latest Security updates applied date were identified of 'Dec 2018' in ICS SITE 1 and 'Dec 2016' in ICS SITE 2. Affected hosts were found to be vulnerable to critical vulnerabilities such as ETERNALBLUE which could result in remote code execution on affected systems.

Recommendation

- Client should consider enforcing and adhering with defined ICS Patch Management Guidelines for applying security patches to operating systems & applications after appropriate testing
- Client should perform periodic vulnerability assessment to identify the status of patches on business critical systems
- …
- …

Evidences:

- Please refer to Appendix

Management Response

Response/Action	Person Responsible	Proposed Completion Date

2.5.5 Inadequate Configuration Management

Finding

It was observed that control systems (i.e. DCS, ESD & F&G) supporting ICS operations are not properly hardened as per Client's hardening standards. The following weaknesses were observed during the fieldwork).

- Server, Engineering/Operator Workstations disk drives are not encrypted.
- Unrestricted PowerShell scripts execution is allowed on the systems.
- Windows Firewall is not enabled on all the ICS Site end hosts.
- BIOS protection is not implemented.

Criticality Rating

Criticality	Ease of Exploitability	Consequences
High	**Possible**	**Major**

Affected System / Devices / URL / Parameter

ICS Site 1	ICS Site 2
• VC9DCSMYT101 • D17DCSEFD101	• D39AMS71001 • D69OWS81001 • D89ESV9D1001

Implication

Unhardened systems or devices can be leveraged by an attacker for privilege escalation by exploiting vulnerable services. The escalated privileges can then be used to alter system configuration facilitating malicious activities. The absence of the proper security configuration results in the execution of malicious PowerShell scripts, programs, usage of unauthorized removable media by an attacker to create a focussed attack.

Recommendation

Client should consider enforcing and adhering with hardening guidelines and vendor operational requirements to determine the settings that allow the necessary system functionality and document exceptions. The following are the recommended configurations related to the fieldwork observation:

- Application whitelisting should be performed
- Scripts execution based on PowerShell, batch file should be restricted.
- Restrict access to Writable CD Media drives (CD-RW) on workstations to end-users in the Control room.
- …
- …
- …

Evidences:

- Please refer to Appendix.

Management Response

Response/Action	Person Responsible	Proposed Completion Date

2.5.6 Outdated Antivirus Definitions

Finding

It was observed that the antivirus (DAT file which contains the updated definitions) is not updated on ICS Site 2 workstation and servers. Updating the offline DAT file usually happens as per vendor availability schedule. ICS Site 2 In scope workstation AV DAT files were updated in <MMM YYYY>.

Criticality Rating

Criticality	Ease of Exploitability	Consequences
Medium	**Possible**	**Moderate**

Affected System / Devices / URL / Parameter

ICS Site 2
• A19ANS81001 • B29QWS81001

Implication

Failing to update antivirus definitions could allow an attacker to execute malicious codes to exploit/ take control of the ICS system supporting business operations and may result in operational disruptions.

Recommendation

- Client should establish procedures to regularly update AV signatures on ICS systems by the vendor. Such procedures should include methods to test, apply and review the updates on ICS systems.
- Client should ensure to take periodic updates from vendor regarding antivirus definations update to identify any missing definations or challenges faced.
- …

Evidences:

- Please refer to Appendix.

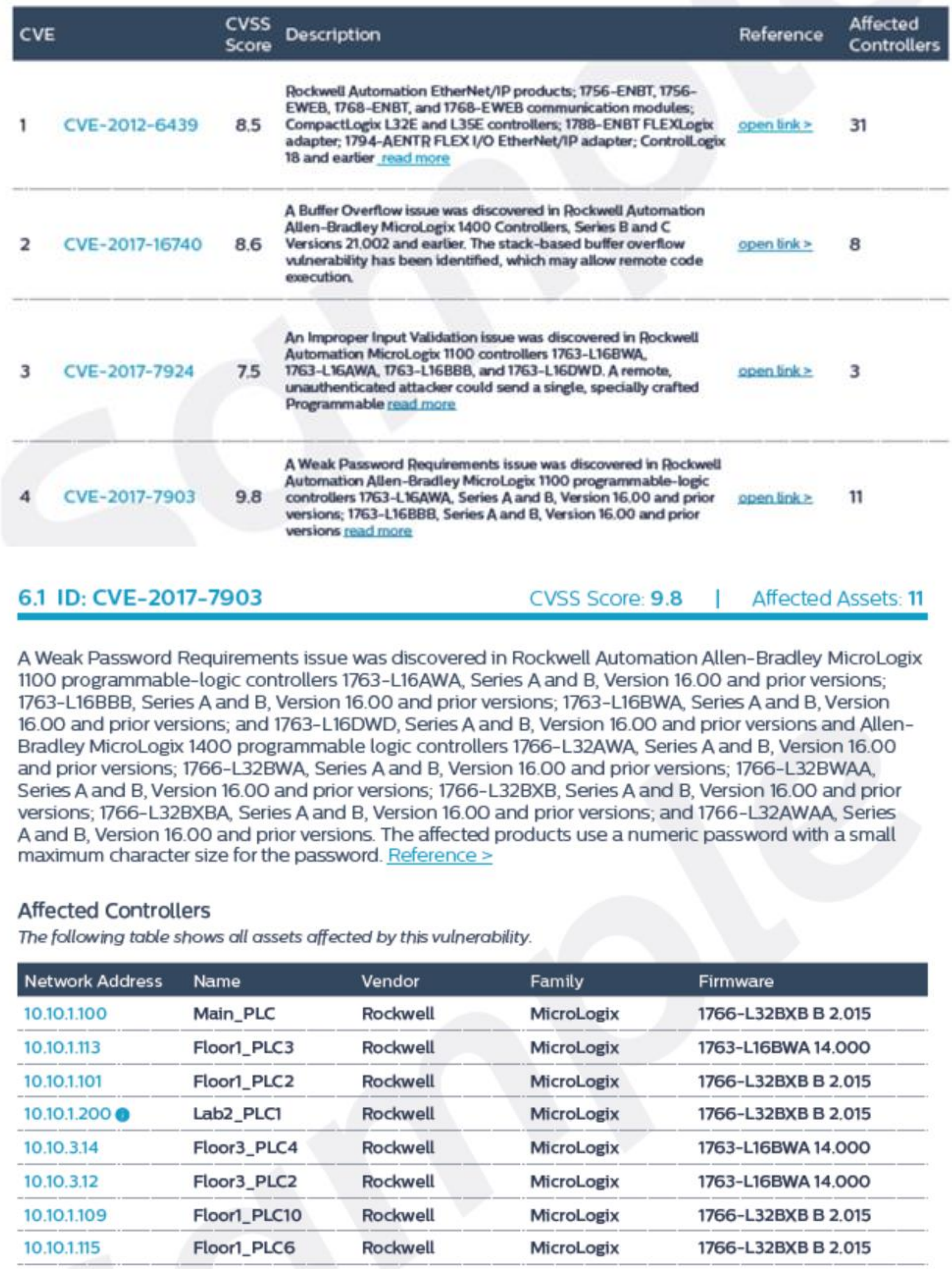
Management Response

Response/Action	Person Responsible	Proposed Completion Date

2.6 Passive Scanning

2.6.1 CVE Details

The following table shows the five most common vulnerabilities in the network. These vulnerabilities affect the highest number of controllers across the environment. Vulnerabilities are ordered by number of affected controllers.



CVE		CVSS Score	Description	Reference	Affected Controllers
1	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 read more	open link >	31
2	CVE-2017-16740	8.6	A Buffer Overflow issue was discovered in Rockwell Automation Allen-Bradley MicroLogix 1400 Controllers, Series B and C Versions 21.002 and earlier. The stack-based buffer overflow vulnerability has been identified, which may allow remote code execution.	open link >	8
3	CVE-2017-7924	7.5	An Improper Input Validation issue was discovered in Rockwell Automation MicroLogix 1100 controllers 1763-L16BWA, 1763-L16AWA, 1763-L16BBB, and 1763-L16DWD. A remote, unauthenticated attacker could send a single, specially crafted Programmable read more	open link >	3
4	CVE-2017-7903	9.8	A Weak Password Requirements issue was discovered in Rockwell Automation Allen-Bradley MicroLogix 1100 programmable-logic controllers 1763-L16AWA, Series A and B, Version 16.00 and prior versions; 1763-L16BBB, Series A and B, Version 16.00 and prior versions read more	open link >	11

6.1 ID: CVE-2017-7903 CVSS Score: 9.8 | Affected Assets: 11

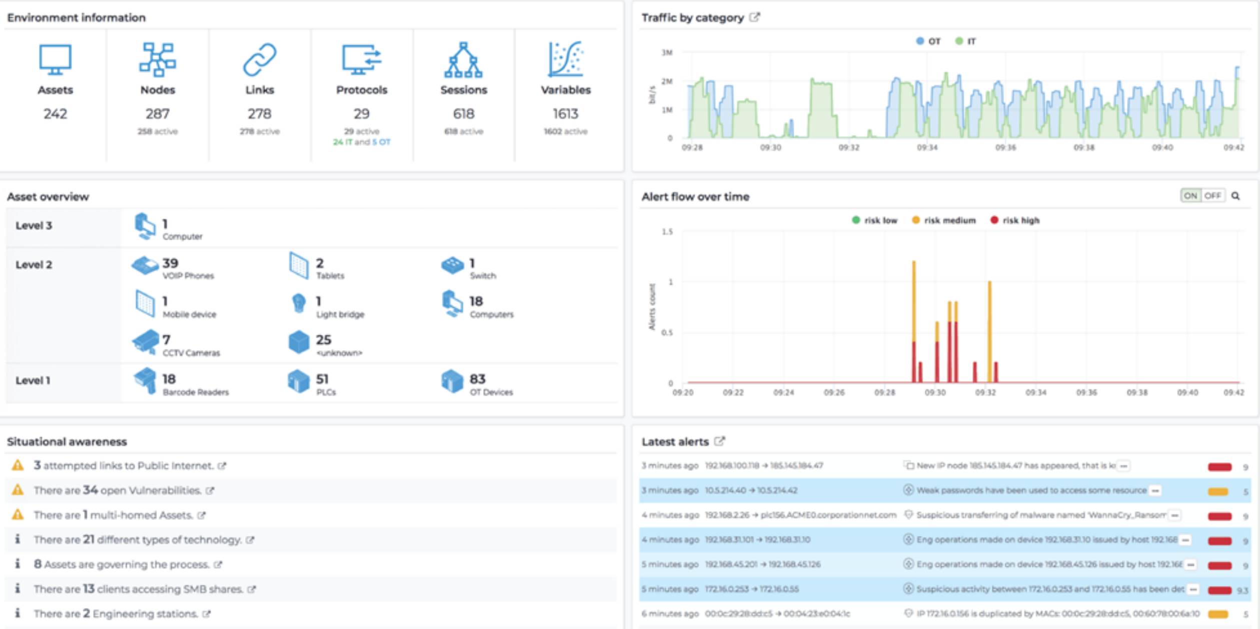
A Weak Password Requirements issue was discovered in Rockwell Automation Allen-Bradley MicroLogix 1100 programmable-logic controllers 1763-L16AWA, Series A and B, Version 16.00 and prior versions; 1763-L16BBB, Series A and B, Version 16.00 and prior versions; 1763-L16BWA, Series A and B, Version 16.00 and prior versions; and 1763-L16DWD, Series A and B, Version 16.00 and prior versions and Allen-Bradley MicroLogix 1400 programmable logic controllers 1766-L32AWA, Series A and B, Version 16.00 and prior versions; 1766-L32BWA, Series A and B, Version 16.00 and prior versions; 1766-L32BWAA, Series A and B, Version 16.00 and prior versions; 1766-L32BXB, Series A and B, Version 16.00 and prior versions; 1766-L32BXBA, Series A and B, Version 16.00 and prior versions; and 1766-L32AWAA, Series A and B, Version 16.00 and prior versions. The affected products use a numeric password with a small maximum character size for the password. Reference >

Affected Controllers

The following table shows all assets affected by this vulnerability.

Network Address	Name	Vendor	Family	Firmware
10.10.1.100	Main_PLC	Rockwell	MicroLogix	1766-L32BXB B 2.015
10.10.1.113	Floor1_PLC3	Rockwell	MicroLogix	1763-L16BWA 14.000
10.10.1.101	Floor1_PLC2	Rockwell	MicroLogix	1766-L32BXB B 2.015
10.10.1.200 ●	Lab2_PLC1	Rockwell	MicroLogix	1766-L32BXB B 2.015
10.10.3.14	Floor3_PLC4	Rockwell	MicroLogix	1763-L16BWA 14.000
10.10.3.12	Floor3_PLC2	Rockwell	MicroLogix	1763-L16BWA 14.000
10.10.1.109	Floor1_PLC10	Rockwell	MicroLogix	1766-L32BXB B 2.015
10.10.1.115	Floor1_PLC6	Rockwell	MicroLogix	1766-L32BXB B 2.015

The Inventory overview section focuses on asset tracking, asset discovery and asset classification. These are the first steps for ensuring operational continuity, reliability and safety. They provide the user with full context for security events and support routine procedures aimed at improving overall cyber hygiene. Creating an inventory for the devices in the network as well as understanding the relationship and connections between them, is a crucial component in the network security.



Environment information

Assets	Nodes	Links	Protocols	Sessions	Variables
242	287 258 active	278 278 active	29 29 active 24 IT and 5 OT	618 618 active	1613 1602 active

Asset overview

Level 3	1 Computer		
Level 2	39 VOIP Phones	2 Tablets	1 Switch
	1 Mobile device	1 Light bridge	18 Computers
	7 CCTV Cameras	25 <unknown>	
Level 1	18 Barcode Readers	51 PLCs	83 OT Devices

Situational awareness

- ⚠ 3 attempted links to Public Internet.
- ⚠ There are 34 open Vulnerabilities.
- ⚠ There are 1 multi-homed Assets.
- ℹ There are 21 different types of technology.
- ℹ 8 Assets are governing the process.
- ℹ There are 13 clients accessing SMB shares.
- ℹ There are 2 Engineering stations.

Traffic by category

Alert flow over time

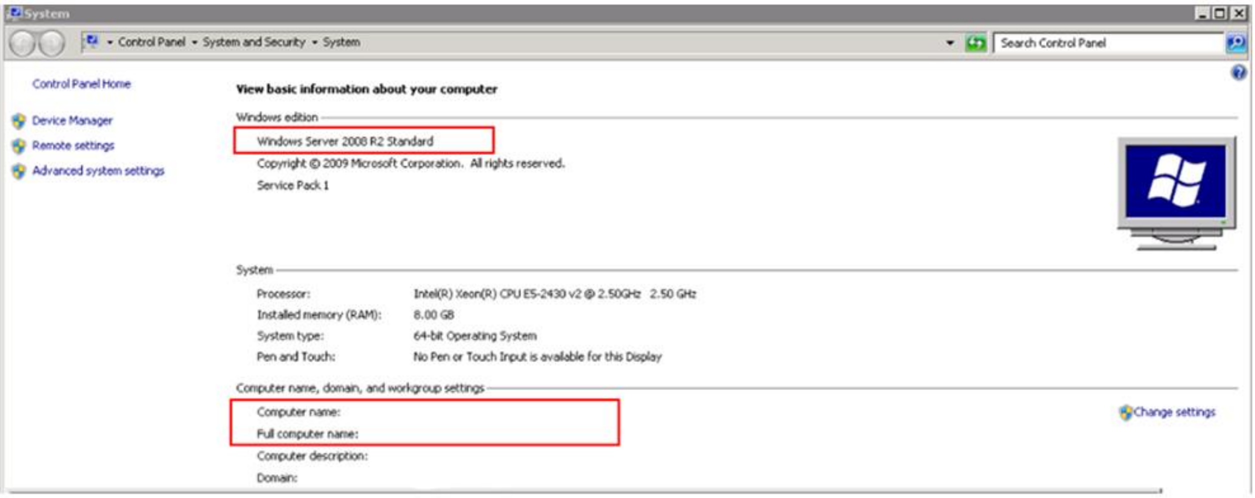
Latest alerts

3 minutes ago	192.168.100.118 → 185.145.184.47	New IP node 185.145.184.47 has appeared, that is kı	🟥	9
3 minutes ago	10.5.214.40 → 10.5.214.42	Weak passwords have been used to access some resource	🟧	5
4 minutes ago	192.168.2.26 → plc156.ACME0.corporationnet.com	Suspicious transferring of malware named 'WannaCry_Ransom	🟥	9
4 minutes ago	192.168.31.101 → 192.168.31.10	Eng operations made on device 192.168.31.10 issued by host 192.168	🟥	9
5 minutes ago	192.168.45.201 → 192.168.45.126	Eng operations made on device 192.168.45.126 issued by host 192.16E	🟥	9
5 minutes ago	172.16.0.253 → 172.16.0.55	Suspicious activity between 172.16.0.253 and 172.16.0.55 has been det	🟥	9.3
6 minutes ago	00:0c:29:28:dd:c5 → 00:04:23:e0:04:1c	IP 172.16.0.156 is duplicated by MACs: 00:0c:29:28:dd:c5, 00:60:78:00:6a:10	🟧	5

3. Appendix

3.1 Evidence Screenshots

3.1.1 Unsupported Operating System and Applications



View basic information about your computer

Windows edition

Windows Server 2008 R2 Standard
Copyright © 2009 Microsoft Corporation. All rights reserved.
Service Pack 1

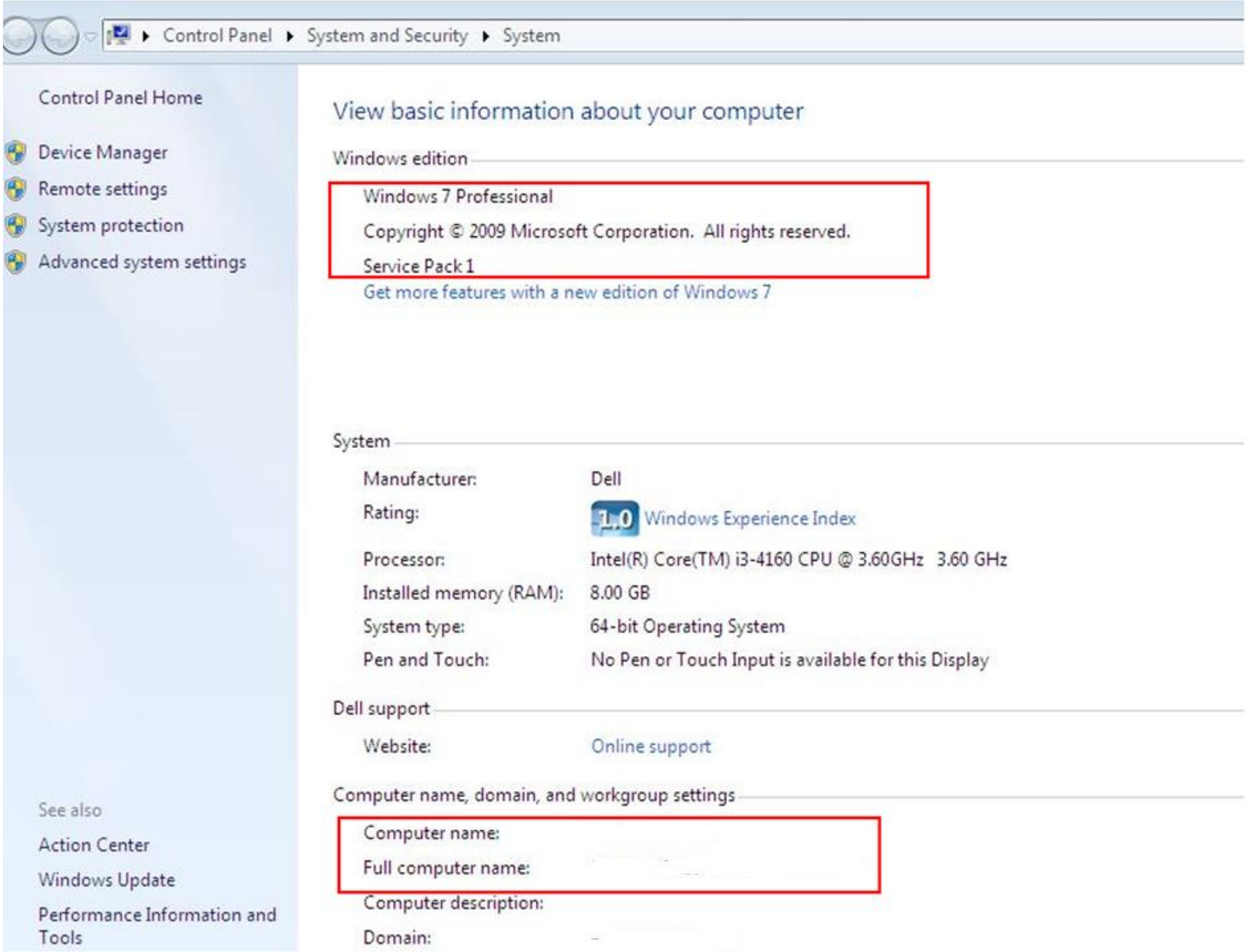
System

Processor:	Intel(R) Xeon(R) CPU E5-2430 v2 @ 2.50GHz 2.50 GHz
Installed memory (RAM):	8.00 GB
System type:	64-bit Operating System
Pen and Touch:	No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name:
Full computer name:
Computer description:
Domain:

Figure 1: Obsolete Operating System



View basic information about your computer

Windows edition

Windows 7 Professional
Copyright © 2009 Microsoft Corporation. All rights reserved.
Service Pack 1
Get more features with a new edition of Windows 7

System

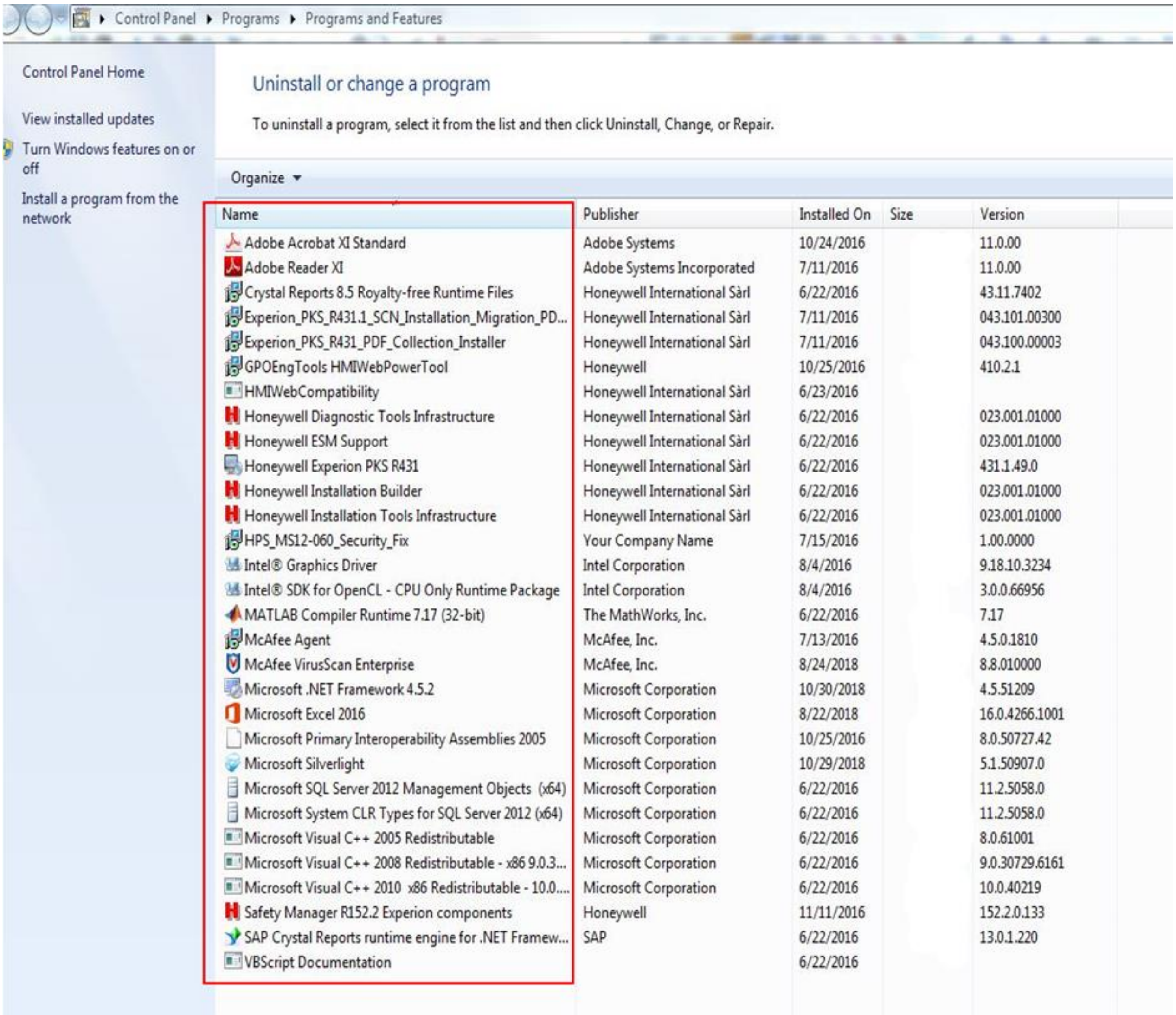
Manufacturer:	Dell
Rating:	1.0 Windows Experience Index
Processor:	Intel(R) Core(TM) i3-4160 CPU @ 3.60GHz 3.60 GHz
Installed memory (RAM):	8.00 GB
System type:	64-bit Operating System
Pen and Touch:	No Pen or Touch Input is available for this Display

Dell support

Website: Online support

Computer name, domain, and workgroup settings

Computer name:
Full computer name:
Computer description:
Domain:



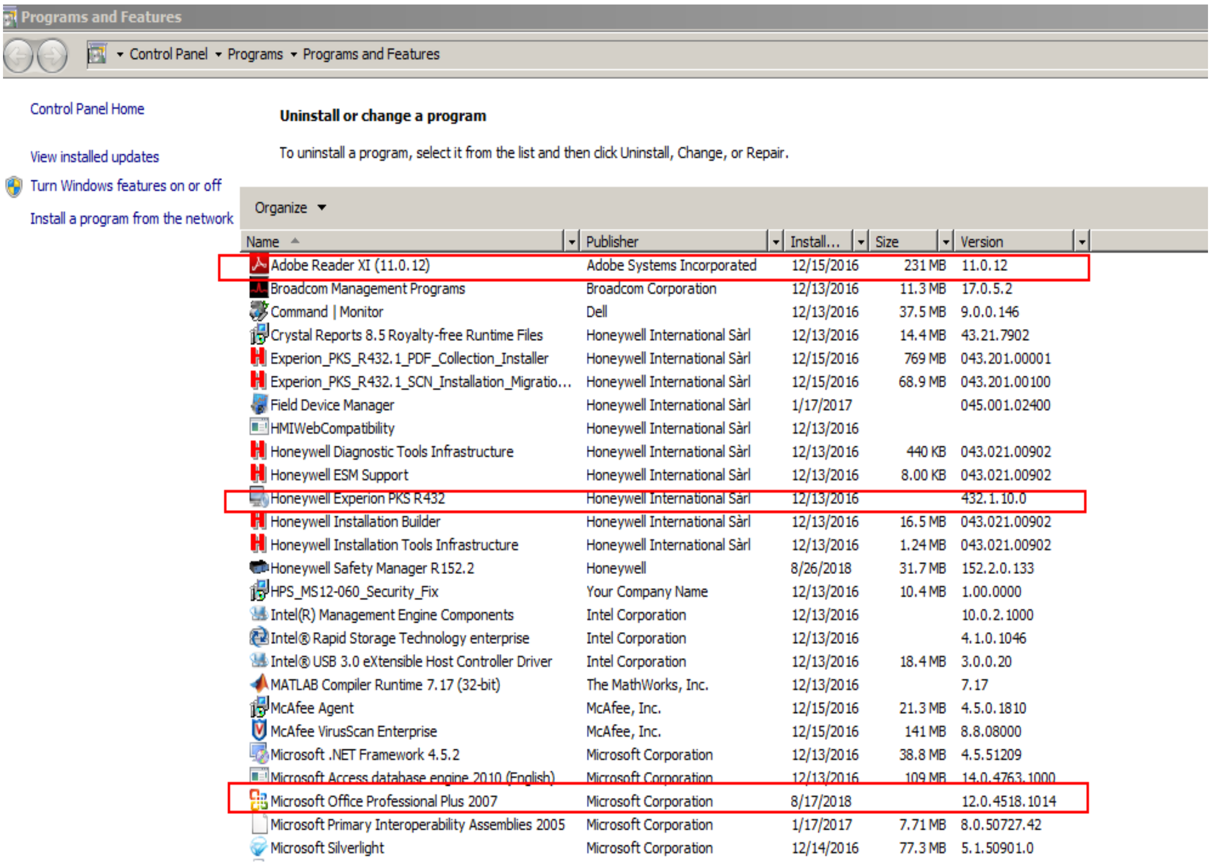
Control Panel ▸ Programs ▸ Programs and Features

Control Panel Home
View installed updates
Turn Windows features on or off
Install a program from the network

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Installed On	Size	Version
Adobe Acrobat XI Standard	Adobe Systems	10/24/2016		11.0.00
Adobe Reader XI	Adobe Systems Incorporated	7/11/2016		11.0.00
Crystal Reports 8.5 Royalty-free Runtime Files	Honeywell International Sàrl	6/22/2016		43.11.7402
Experion_PKS_R431.1_SCN_Installation_Migration_PD...	Honeywell International Sàrl	7/11/2016		043.101.00300
Experion_PKS_R431_PDF_Collection_Installer	Honeywell International Sàrl	7/11/2016		043.100.00003
GPOEngTools HMIWebPowerTool	Honeywell	10/25/2016		410.2.1
HMIWebCompatibility	Honeywell International Sàrl	6/23/2016		
Honeywell Diagnostic Tools Infrastructure	Honeywell International Sàrl	6/22/2016		023.001.01000
Honeywell ESM Support	Honeywell International Sàrl	6/22/2016		023.001.01000
Honeywell Experion PKS R431	Honeywell International Sàrl	6/22/2016		431.1.49.0
Honeywell Installation Builder	Honeywell International Sàrl	6/22/2016		023.001.01000
Honeywell Installation Tools Infrastructure	Honeywell International Sàrl	6/22/2016		023.001.01000
HPS_MS12-060_Security_Fix	Your Company Name	7/15/2016		1.00.0000
Intel® Graphics Driver	Intel Corporation	8/4/2016		9.18.10.3234
Intel® SDK for OpenCL - CPU Only Runtime Package	Intel Corporation	8/4/2016		3.0.0.66956
MATLAB Compiler Runtime 7.17 (32-bit)	The MathWorks, Inc.	6/22/2016		7.17
McAfee Agent	McAfee, Inc.	7/13/2016		4.5.0.1810
McAfee VirusScan Enterprise	McAfee, Inc.	8/24/2018		8.8.010000
Microsoft .NET Framework 4.5.2	Microsoft Corporation	10/30/2018		4.5.51209
Microsoft Excel 2016	Microsoft Corporation	8/22/2018		16.0.4266.1001
Microsoft Primary Interoperability Assemblies 2005	Microsoft Corporation	10/25/2016		8.0.50727.42
Microsoft Silverlight	Microsoft Corporation	10/29/2018		5.1.50907.0
Microsoft SQL Server 2012 Management Objects (x64)	Microsoft Corporation	6/22/2016		11.2.5058.0
Microsoft System CLR Types for SQL Server 2012 (x64)	Microsoft Corporation	6/22/2016		11.2.5058.0
Microsoft Visual C++ 2005 Redistributable	Microsoft Corporation	6/22/2016		8.0.61001
Microsoft Visual C++ 2008 Redistributable - x86 9.0.3...	Microsoft Corporation	6/22/2016		9.0.30729.6161
Microsoft Visual C++ 2010 x86 Redistributable - 10.0....	Microsoft Corporation	6/22/2016		10.0.40219
Safety Manager R152.2 Experion components	Honeywell	11/11/2016		152.2.0.133
SAP Crystal Reports runtime engine for .NET Framew...	SAP	6/22/2016		13.0.1.220
VBScript Documentation		6/22/2016		



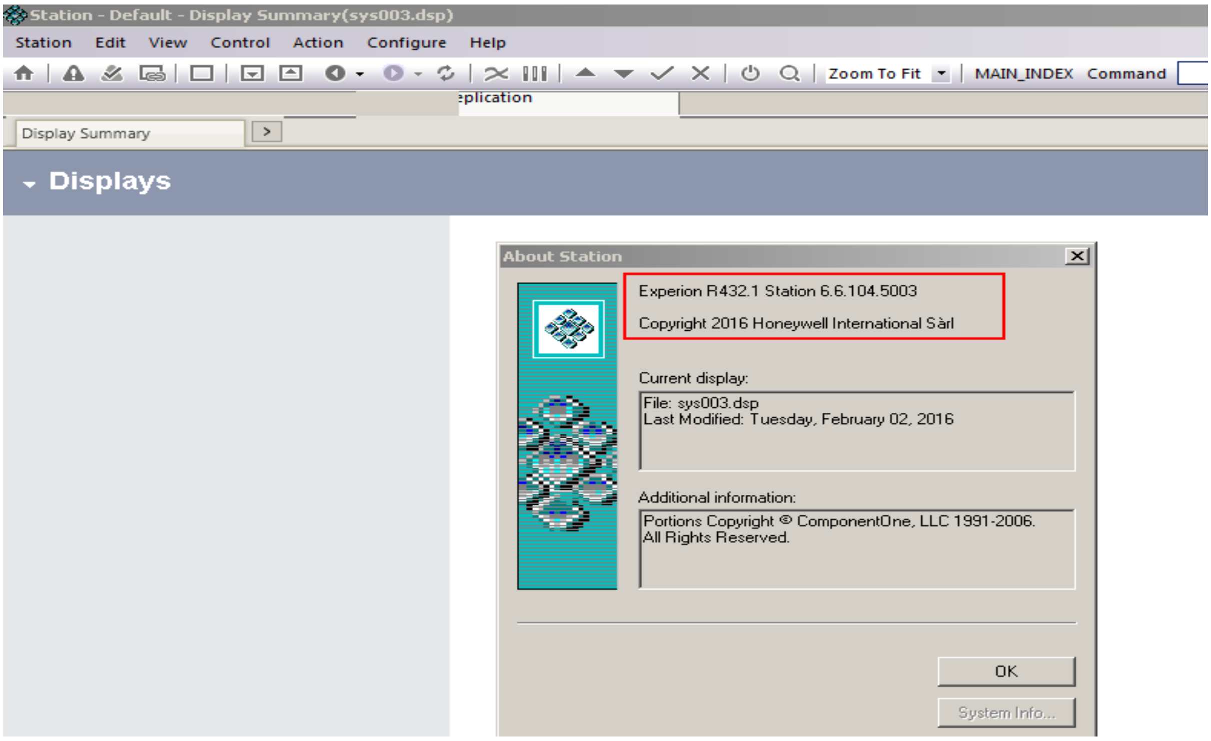
Programs and Features
Control Panel ▸ Programs ▸ Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Install a program from the network
Organize ▾

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Install...	Size	Version
Adobe Reader XI (11.0.12)	Adobe Systems Incorporated	12/15/2016	231 MB	11.0.12
Broadcom Management Programs	Broadcom Corporation	12/13/2016	11.3 MB	17.0.5.2
Command | Monitor	Dell	12/13/2016	37.5 MB	9.0.0.146
Crystal Reports 8.5 Royalty-free Runtime Files	Honeywell International Sàrl	12/13/2016	14.4 MB	43.21.7902
Experion_PKS_R432.1_PDF_Collection_Installer	Honeywell International Sàrl	12/15/2016	769 MB	043.201.00001
Experion_PKS_R432.1_SCN_Installation_Migratio...	Honeywell International Sàrl	12/15/2016	68.9 MB	043.201.00100
Field Device Manager	Honeywell International Sàrl	1/17/2017		045.001.02400
HMIWebCompatibility	Honeywell International Sàrl	12/13/2016		
Honeywell Diagnostic Tools Infrastructure	Honeywell International Sàrl	12/13/2016	440 KB	043.021.00902
Honeywell ESM Support	Honeywell International Sàrl	12/13/2016	8.00 KB	043.021.00902
Honeywell Experion PKS R432	Honeywell International Sàrl	12/13/2016		432.1.10.0
Honeywell Installation Builder	Honeywell International Sàrl	12/13/2016	16.5 MB	043.021.00902
Honeywell Installation Tools Infrastructure	Honeywell International Sàrl	12/13/2016	1.24 MB	043.021.00902
Honeywell Safety Manager R152.2	Honeywell	8/26/2018	31.7 MB	152.2.0.133
HPS_MS12-060_Security_Fix	Your Company Name	12/13/2016	10.4 MB	1.00.0000
Intel(R) Management Engine Components	Intel Corporation	12/13/2016		10.0.2.1000
Intel® Rapid Storage Technology enterprise	Intel Corporation	12/13/2016		4.1.0.1046
Intel® USB 3.0 eXtensible Host Controller Driver	Intel Corporation	12/13/2016	18.4 MB	3.0.0.20
MATLAB Compiler Runtime 7.17 (32-bit)	The MathWorks, Inc.	12/13/2016		7.17
McAfee Agent	McAfee, Inc.	12/15/2016	21.3 MB	4.5.0.1810
McAfee VirusScan Enterprise	McAfee, Inc.	12/15/2016	141 MB	8.8.08000
Microsoft .NET Framework 4.5.2	Microsoft Corporation	12/13/2016	38.8 MB	4.5.51209
Microsoft Access database engine 2010 (English)	Microsoft Corporation	12/13/2016	109 MB	14.0.4763.1000
Microsoft Office Professional Plus 2007	Microsoft Corporation	8/17/2018		12.0.4518.1014
Microsoft Primary Interoperability Assemblies 2005	Microsoft Corporation	1/17/2017	7.71 MB	8.0.50727.42
Microsoft Silverlight	Microsoft Corporation	12/14/2016	77.3 MB	5.1.50901.0

Figure 2: Outdated Software's on Workstations



Experion R432.1 Station 6.6.104.5003

Copyright 2016 Honeywell International Sàrl

Current display:

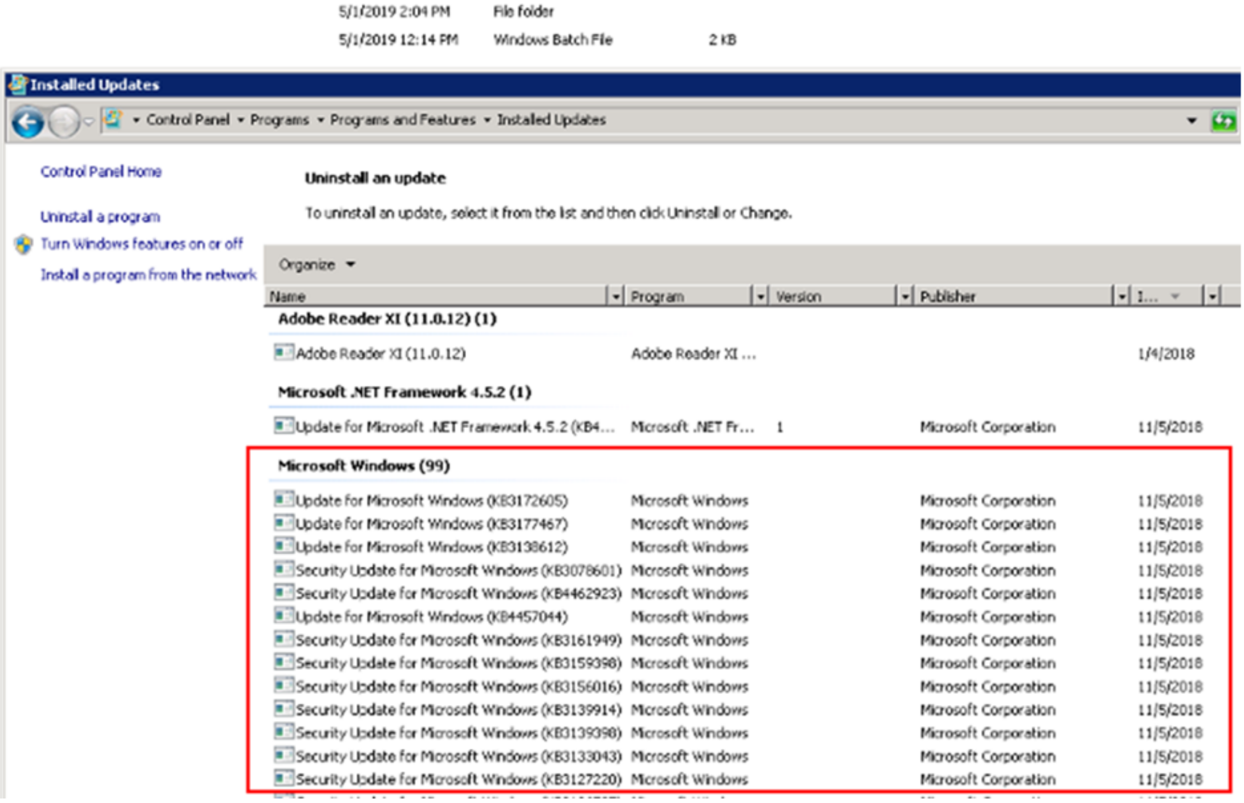
File: sys003.dsp
Last Modified: Tuesday, February 02, 2016

Additional information:

Portions Copyright © ComponentOne, LLC 1991-2006.
All Rights Reserved.

Figure 3: Honeywell Experion station application

3.1.2 Inadequate Patch Management



5/1/2019 2:04 PM File folder
5/1/2019 12:14 PM Windows Batch File 2 KB

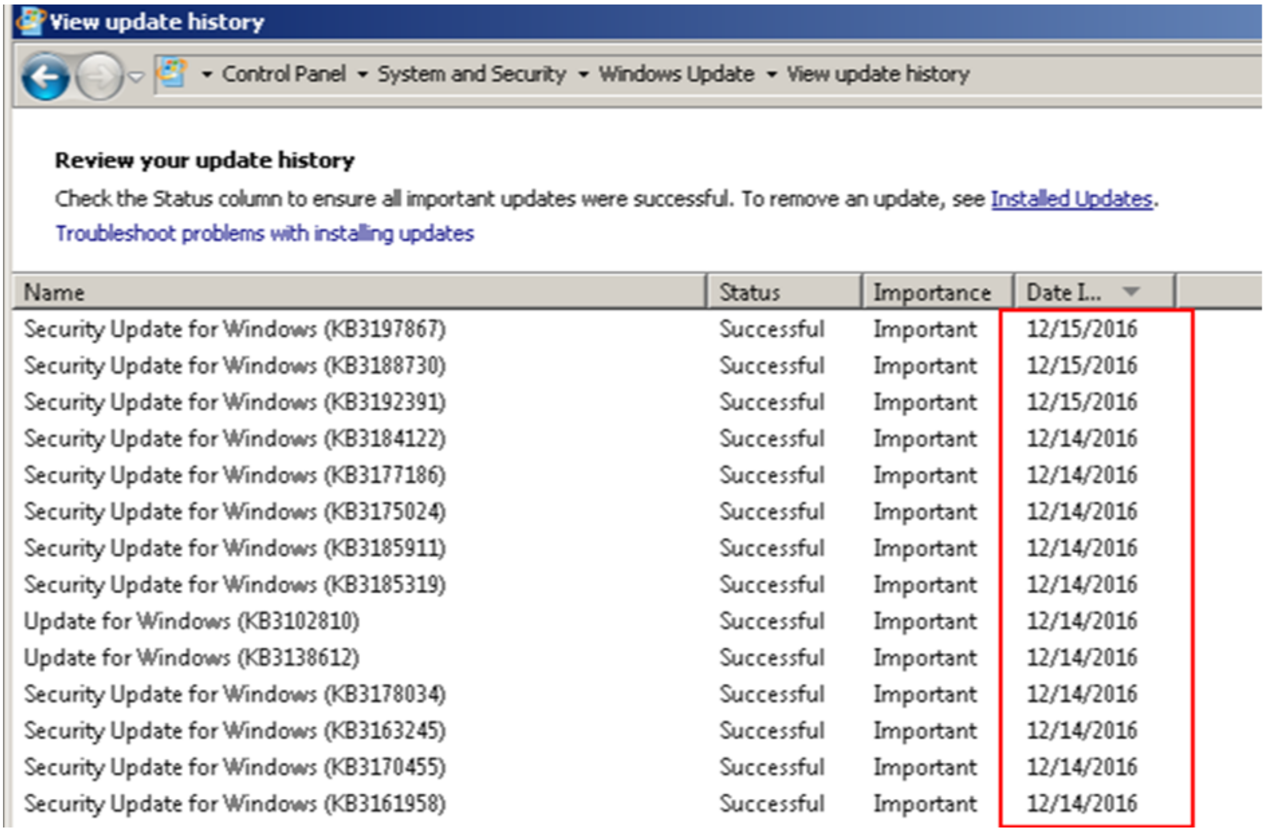
Installed Updates

Control Panel ▸ Programs ▸ Programs and Features ▸ Installed Updates
Control Panel Home
Uninstall a program
Turn Windows features on or off
Install a program from the network
Organize ▾

Uninstall an update

To uninstall an update, select it from the list and then click Uninstall or Change.

Name	Program	Version	Publisher	I...
Adobe Reader XI (11.0.12) (1)				
Adobe Reader XI (11.0.12)	Adobe Reader XI ...			1/4/2018
Microsoft .NET Framework 4.5.2 (1)				
Update for Microsoft .NET Framework 4.5.2 (KB4...	Microsoft .NET Fr...	1	Microsoft Corporation	11/5/2018
Microsoft Windows (99)				
Update for Microsoft Windows (KB3172605)	Microsoft Windows		Microsoft Corporation	11/5/2018
Update for Microsoft Windows (KB3177467)	Microsoft Windows		Microsoft Corporation	11/5/2018
Update for Microsoft Windows (KB3138612)	Microsoft Windows		Microsoft Corporation	11/5/2018
Security Update for Microsoft Windows (KB3078601)	Microsoft Windows		Microsoft Corporation	11/5/2018
Security Update for Microsoft Windows (KB4462923)	Microsoft Windows		Microsoft Corporation	11/5/2018
Update for Microsoft Windows (KB4457044)	Microsoft Windows		Microsoft Corporation	11/5/2018
Security Update for Microsoft Windows (KB3161949)	Microsoft Windows		Microsoft Corporation	11/5/2018
Security Update for Microsoft Windows (KB3159398)	Microsoft Windows		Microsoft Corporation	11/5/2018
Security Update for Microsoft Windows (KB3156016)	Microsoft Windows		Microsoft Corporation	11/5/2018
Security Update for Microsoft Windows (KB3139914)	Microsoft Windows		Microsoft Corporation	11/5/2018
Security Update for Microsoft Windows (KB3139398)	Microsoft Windows		Microsoft Corporation	11/5/2018
Security Update for Microsoft Windows (KB3133043)	Microsoft Windows		Microsoft Corporation	11/5/2018
Security Update for Microsoft Windows (KB3127220)	Microsoft Windows		Microsoft Corporation	11/5/2018



View update history

Control Panel ▸ System and Security ▸ Windows Update ▸ View update history

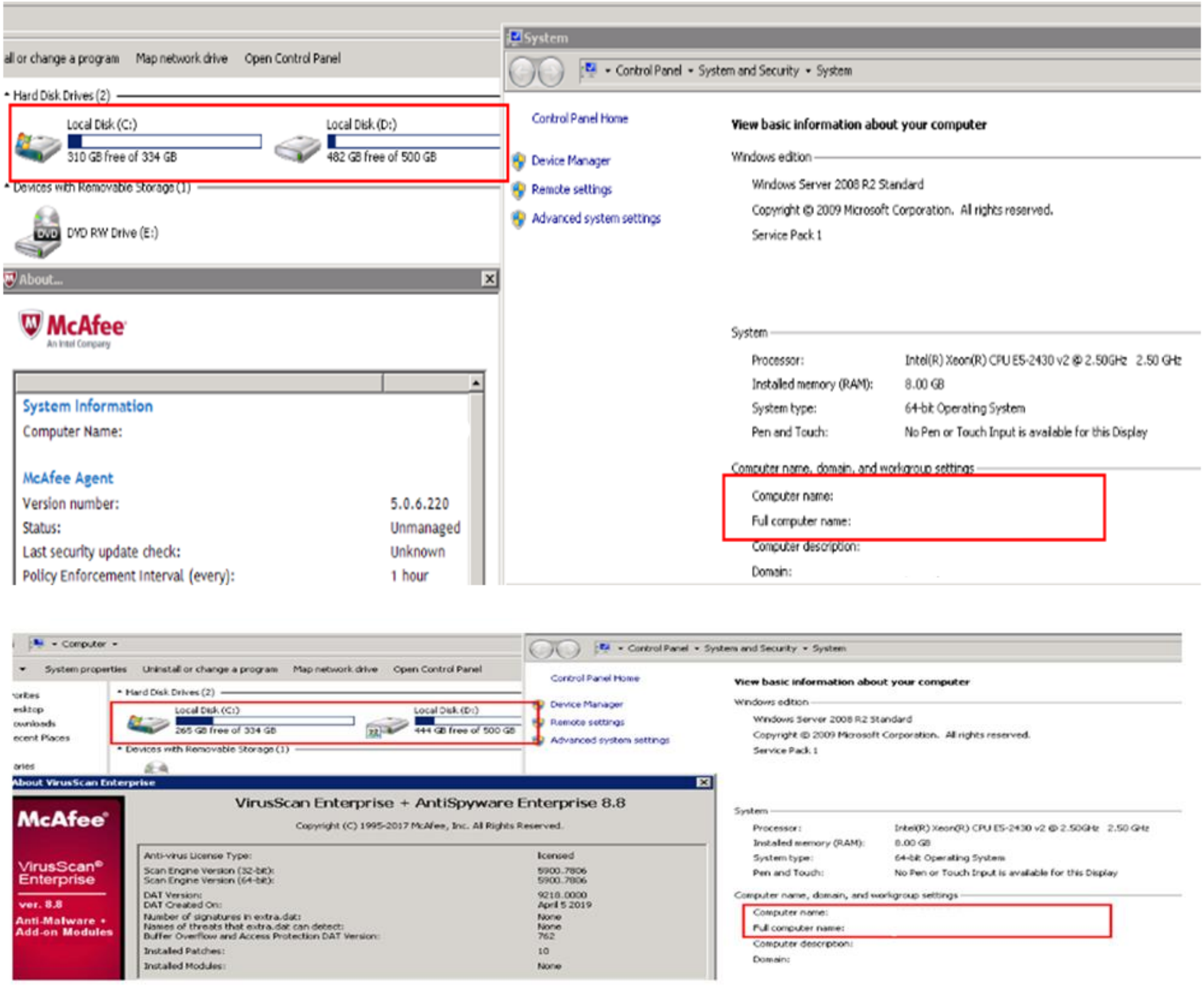
Review your update history

Check the Status column to ensure all important updates were successful. To remove an update, see Installed Updates.

Troubleshoot problems with installing updates

Name	Status	Importance	Date I...
Security Update for Windows (KB3197867)	Successful	Important	12/15/2016
Security Update for Windows (KB3188730)	Successful	Important	12/15/2016
Security Update for Windows (KB3192391)	Successful	Important	12/15/2016
Security Update for Windows (KB3184122)	Successful	Important	12/14/2016
Security Update for Windows (KB3177186)	Successful	Important	12/14/2016
Security Update for Windows (KB3175024)	Successful	Important	12/14/2016
Security Update for Windows (KB3185911)	Successful	Important	12/14/2016
Security Update for Windows (KB3185319)	Successful	Important	12/14/2016
Update for Windows (KB3102810)	Successful	Important	12/14/2016
Update for Windows (KB3138612)	Successful	Important	12/14/2016
Security Update for Windows (KB3178034)	Successful	Important	12/14/2016
Security Update for Windows (KB3163245)	Successful	Important	12/14/2016
Security Update for Windows (KB3170455)	Successful	Important	12/14/2016
Security Update for Windows (KB3161958)	Successful	Important	12/14/2016

3.1.3 Inadequate Configuration Management



Local Disk (C:) 310 GB free of 334 GB

Local Disk (D:) 482 GB free of 500 GB

System Information

Computer Name:

McAfee Agent

```
Version number:                          5.0.6.220
Status:                                  Unmanaged
Last security update check:              Unknown
Policy Enforcement Interval (every):     1 hour
```

View basic information about your computer

Windows edition

Windows Server 2008 R2 Standard

Copyright © 2009 Microsoft Corporation. All rights reserved.

Service Pack 1

System

```
Processor:               Intel(R) Xeon(R) CPU E5-2430 v2 @ 2.50GHz   2.50 GHz
Installed memory (RAM):  8.00 GB
System type:             64-bit Operating System
Pen and Touch:           No Pen or Touch Input is available for this Display
```

Computer name, domain, and workgroup settings

```
Computer name:
Full computer name:
Computer description:
Domain:
```

Local Disk (C:) 265 GB free of 334 GB

Local Disk (D:) 444 GB free of 500 GB

VirusScan Enterprise + AntiSpyware Enterprise 8.8

Copyright (C) 1995-2017 McAfee, Inc. All Rights Reserved.

```
Anti-virus License Type:                                  licensed
Scan Engine Version (32-bit):                             5900.7806
Scan Engine Version (64-bit):                             5900.7806
DAT Version:                                              9218.0000
DAT Created On:                                           April 5 2019
Number of signatures in extra.dat:                        None
Names of threats that extra.dat can detect:               None
Buffer Overflow and Access Protection DAT Version:        762
Installed Patches:                                        10
Installed Modules:                                        None
```

View basic information about your computer

Windows edition

Windows Server 2008 R2 Standard

Copyright © 2009 Microsoft Corporation. All rights reserved.

Service Pack 1

System

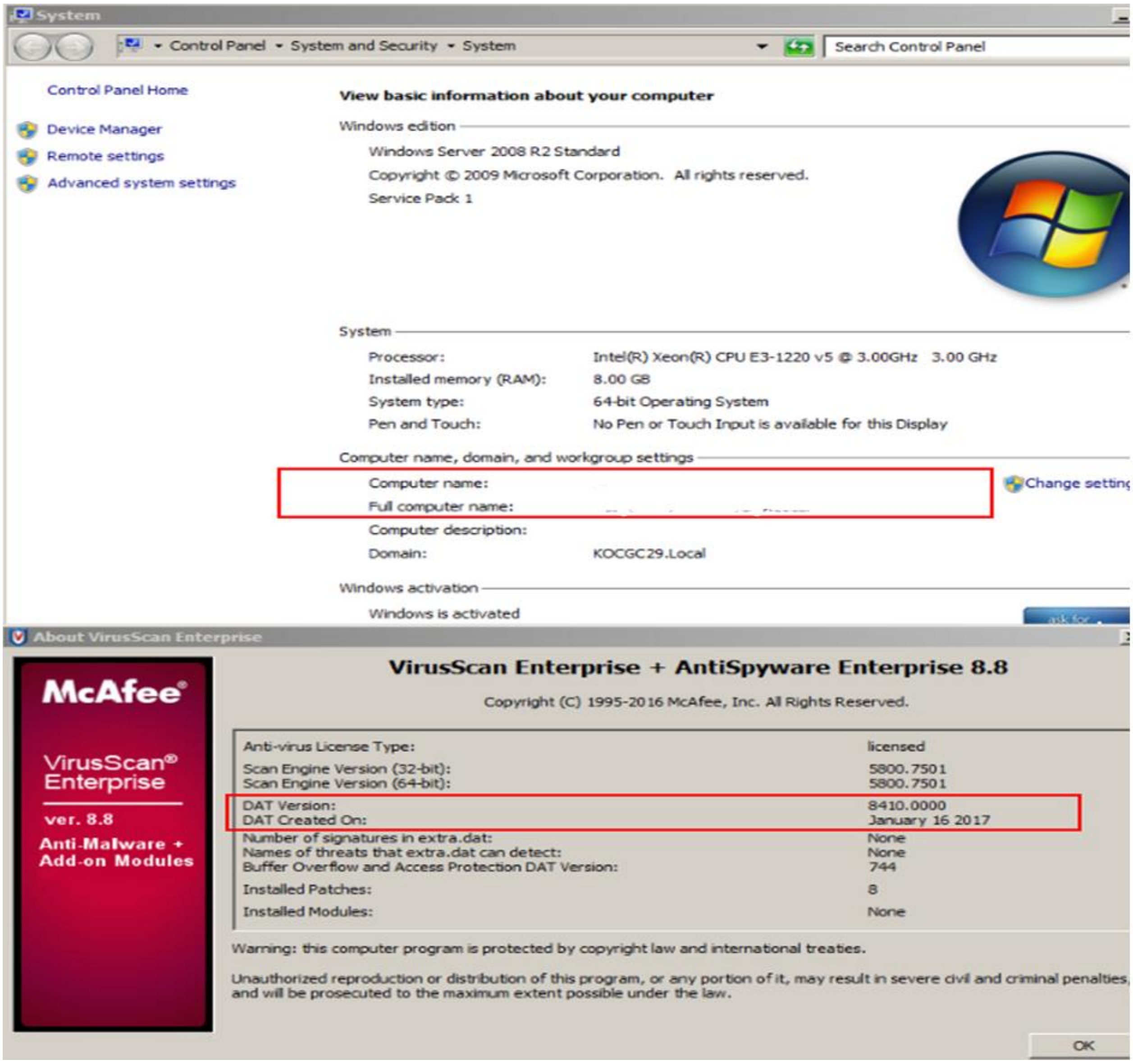
```
Processor:               Intel(R) Xeon(R) CPU E5-2430 v2 @ 2.50GHz   2.50 GHz
Installed memory (RAM):  8.00 GB
System type:             64-bit Operating System
Pen and Touch:           No Pen or Touch Input is available for this Display
```

Computer name, domain, and workgroup settings

```
Computer name:
Full computer name:
Computer description:
Domain:
```

Figure 4: Bit locker encryption is not enabled

3.1.4 Outdated Antivirus Definitions



View basic information about your computer

Windows edition

Windows Server 2008 R2 Standard
Copyright © 2009 Microsoft Corporation. All rights reserved.
Service Pack 1

System

Processor:	Intel(R) Xeon(R) CPU E3-1220 v5 @ 3.00GHz 3.00 GHz
Installed memory (RAM):	8.00 GB
System type:	64-bit Operating System
Pen and Touch:	No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name:	
Full computer name:	
Computer description:	
Domain:	KOCGC29.Local

Windows activation

Windows is activated

VirusScan Enterprise + AntiSpyware Enterprise 8.8

Copyright (C) 1995-2016 McAfee, Inc. All Rights Reserved.

Anti-virus License Type:	licensed
Scan Engine Version (32-bit):	5800.7501
Scan Engine Version (64-bit):	5800.7501
DAT Version:	8410.0000
DAT Created On:	January 16 2017
Number of signatures in extra.dat:	None
Names of threats that extra.dat can detect:	None
Buffer Overflow and Access Protection DAT Version:	744
Installed Patches:	8
Installed Modules:	None

Warning: this computer program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

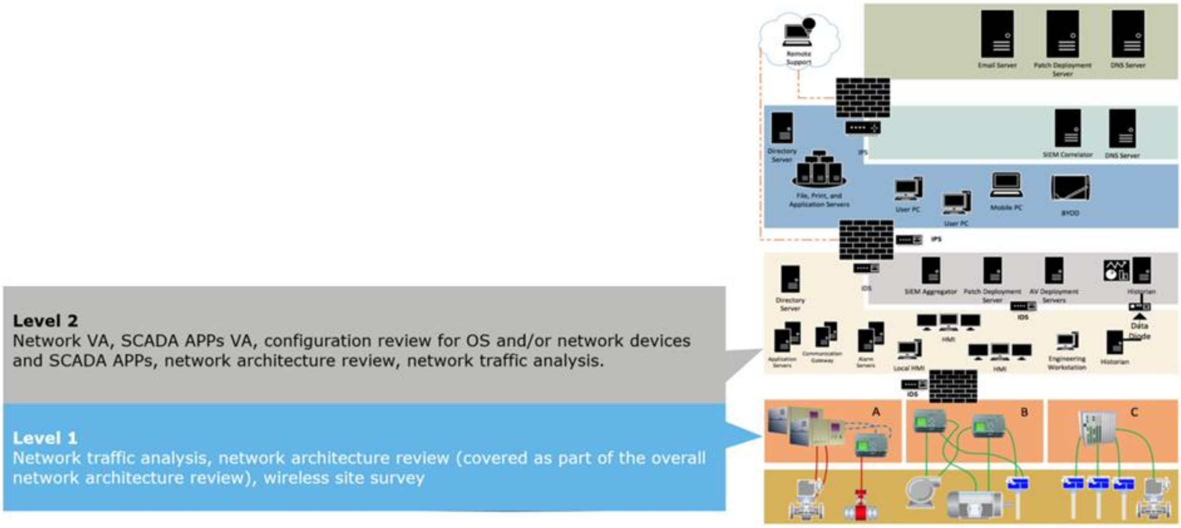
Figure 5: ICS SITE outdated DAT

3.2 Client's ICS Guidelines and Standards

<Provide References to Client's standards & Guidelines Here>

3.3 OT Assessment Approach followed

Client's ICS security assessment scope and review involved testing a number of areas based on the standard ICS segmentation model. Only level one, level two will be considered in the scope. Below is the mapping of activities per level:



Level 2
Network VA, SCADA APPs VA, configuration review for OS and/or network devices and SCADA APPs, network architecture review, network traffic analysis.

Level 1
Network traffic analysis, network architecture review (covered as part of the overall network architecture review), wireless site survey

3.3.1 Maturity Review, Risk Based Approach, Passive Scanning & Config Reviews

Payatu uses Interview based approach for Maturity Review and Risk Based Approach. For Passive scanning a wide variety of tools are used depending on the environment to be assessed. It is vital that the production environment is not impacted during the review process.

Depending on scope and the nature of the target system the following methods could be used:

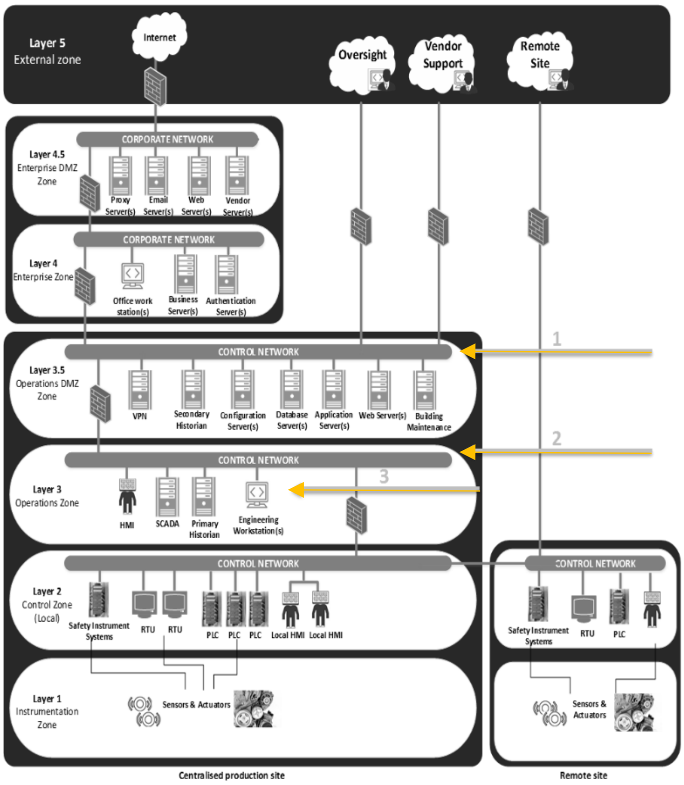
- Manual configuration inspection;
- Extraction of system configuration for offline analysis;
- Execution of system utilities (with administrative access) and extracting output for offline analysis;
- Installation and execution of scripted or binary programs (with administrative access) and extracting output for offline analysis.

For Passive scanning the output is analyzed, Payatu will rationalize it, removing inconsistencies, irrelevant information and false positives.

To facilitate the tests, the team uses a combination of open source and / commercial tools, based on the operating system technology & version and a set of scripts.

3.3.2 Network Architecture Assessment

Below mentioned activities are performed as part of a secure network architecture review at ICS sites:



- Interviews with personnel to assess the maturity of security processes in the control domain.
- An external security test to assess the site internet-facing assets (arrow 1);
- An internal infrastructure security test to assess the possibility to access the operational network through the office network (arrow 2); and Configuration security test and ICS software review to test the current level of security of the operational environment (arrow 3).
- Network Traffic Analysis: Payatu will select key network choke points that will be subject to network traffic analysis using platform-specific security diagnostic tools and techniques. The objective is to assess if the traffic contains malicious behavior and elevate any persistence incidents, in addition to identifying unauthorized systems per level and suspicious network flows.

3.3.3 Network Layer Zone descriptions:

Layer 5: External Zone: transfer connection and information to third parties

Layer 4.5: Demilitarized Enterprise Zone: Contains proxy server(s), email server(s), web server(S) and vendor management server(s)

Layer 4: Enterprise Zone: Contains enterprise IT & common services

Layer 3.5: Demilitarized Operations Zone: Contains multiple servers such as secondary historian server(s), configuration server(s), and database server.

Layer 3: Operations Zone: Contains primary historian server(s), ICS server(s), engineering workstation(s) and HMI

Layer 2: Local Control Zone: Contains physical field devices (PLCs, RTUs and local HMI

Layer 1: Instrumentation Zone: Contains sensors and actuators

End of Report