OT/ IoT Vulnerability Assessment Sample Report

Table of Contents

Contents

Copyright

Disclaimer

By accessing and using this report you agree to the following terms and conditions and all applicable laws, without limitation or qualification, unless otherwise stated, the contents of this document including, but not limited to, the text and images contained herein and their arrangement are the property of Infopercept Consulting Pvt Ltd (Infopercept). Nothing contained in this document shall be construed as conferring by implication, estoppel, or otherwise, any license or right to any copyright, patent, trademark or other proprietary interest of Infopercept or any third party. This document and its contents including, but not limited to, graphic images and documentation may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, without the prior written consent of Infopercept. Any use you make of the information provided, is at your own risk and liability. Infopercept makes no representation about the suitability, reliability, availability, timeliness, and accuracy of the information, products, services, and related graphics contained in this document. All such information products, services, related graphics and other contents are provided 'as is' without warranty of any kind. The relationship between you and Infopercept shall be governed by the laws of the Republic of India without regard to its conflict of law provisions. You and Infopercept agree to submit to the personal and exclusive jurisdiction of the courts located at Mumbai, India. You are responsible for complying with the laws of the jurisdiction and agree that you will not access or use the information in this report, in violation of such laws. You represent that you have the lawful right to submit such information and agree that you will not submit any information unless you are legally entitled to do so.

Overview

ABC Company Ltd. has appointed Infopercept Consulting Pvt. Ltd. a multidisciplinary company specializing in information OT/IoT security assessments to review its Network, with a perspective of evaluating the effectiveness of the technical controls by following ethical hacking procedures.

The information contained in this report is confidential and is intended only for use by the management of ABC Company Ltd. Outsourcing Services. We are not responsible to any other person/ party or for any decision of such person or party based on this report. It is hereby notified that any reproduction, copying or otherwise quoting of this report or any part thereof except for the purpose mentioned herein above can be done only with our prior written permission.

Detailed Vulnerability Information Sources of Information

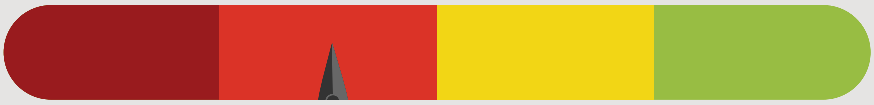
We have called for and obtained such data, information etc. as were necessary for the purpose of our assignment which has been made available to us by the management or been found in the public domain.

The information relating to the server details, ip-address, network devices, configuration etc. has been obtained from the Information Technology Team.

Summary of Findings

The graph below shows a summary of the number of vulnerabilities found for each impact level for the Assessment. A significant number of high impact vulnerabilities were found that should be addressed as a priority.

Risk Level	CRITICAL	HIGH	MEDIUM	LOW



Risk Count	0	1	1	1
Total – 3				

1.Report Format

Vulnerability assessment was carried out for each IP/Address/URL listed in scope. The discovered vulnerabilities are arranged per host, beginning with the host information followed by the vulnerabilities for that system. Below is a description of how the vulnerabilities per IP/Address/URL are listed: -

IP: xxx.x.xx

URL: abccorporation.com

Vulnerability Information:

Compliance of IP Address:	
Risk	
Abstract	
IPMG Control Violation	
Reference	
Ease of Exploitation	
Impact	
Recommendations	

Vulnerability Title

A short title that describes the vulnerability.

For each vulnerability, the title bar is color coded for a quick identification of the risk level. Title bar color codes are as follows:

Risk Level & Color Code :

CRITICAL

HIGH

MEDIUM

LOW

INFORMATION

EXTERNALLY

- Abstract - Describes the flaw or bugs that cause the vulnerability
- IPMG Control Violation- Provides the ABC IPMG control numbers that are violated.
- Reference- Describes the reference for the respective vulnerability found.
- Ease of Exploitation- Provides a metric for the skill level required to exploit the vulnerability.

Metric Skill-level	Metric Skill-level
Easy	Casual user
Medium	Computer-savvy individual
Hard	Determined hacker

The categories are:

- Impact- Describes the possible business impact to ABC if this vulnerability is successfully exploited by an attacker.
- Recommendation- Provides solutions or workarounds to mitigate the risk arising from this vulnerability.
- Proof of Concept- Screenshots / supporting evidence showing the vulnerability being exploited.

2. OT/ IoT Vulnerability Assessment Report

For the Internal Vulnerability Assessment of the Industrial Internet of Things (IIOT), below are the in-scope targets that were chosen by ABC Corporation Engineering Team. These targets represented and resembled ABC Corporation’s two different setups on-site. Due to the criticality of the system and agreement with the ABC Corporation’s Engineering Team, assessment was carried on these targets as they had available spare setup, which were identical to the working setup.

NO.	IP/Address/URL
1.	10.10.10.1 (Mixer HMI)
2.	10.10.10.5 (Mixer PLC)
3.	10.0.0.2 (Bread Cooler HMI)
4.	10.0.0.1 (Bread Cooler PLC)

No.	Finding	Affected IP(s) / Status	Impact	Recommendations	Management Response
Risk rating: High Risk					
GBKL.TA. IIOT.1	Anonymous File Upload Enabled Executive Summary: During the assessment, we noted that it is possible to upload a file to the device without providing any credentials. Technical Summary: During the assessment we noted that the remote FTP server allows anonymous logins. Anonymous FTP allows users without accounts to have access to certain directories on the system.	OPEN 10.10.10.1:21 10.0.0.2:21	Business Impact: An attacker can upload his code to the device which this code can be run offline and changes the configuration of the device, causing the production line malfunctioning, hence interrupting the production line and damaging the device or disrupting the manufacturing which leads to business loss. Technical Impact: An attacker could have access to certain directories on the system, and upload malicious code to the device and run this code at a later time while offline to change configuration of HMI and leading to malfunctioning of PLC and attached machinery.	If you are not using this service, it is recommended to disable it or at least deny anonymous logins	

No.	Finding	Affected IP(s) / Status	Impact	Recommendations	Management Response
Risk rating: Low Risk Risk					
GBKL.TA.IIOT.3	Message Signing Disabled Executive Summary: During the assessment, we noted that messages between parts of machinery are not signed to ensure the validity of origin or sender. Technical Summary: During the assessment, we noted that signing is not required on the remote SMB server.	OPEN 10.0.0.2:445	Business Impact: Since the data is not signed properly while transmitted to the destination, an attacker can take advantage of this vulnerability to intercept the line and get unauthorized access to the information being transmitted to the destination. Technical Impact: An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.	Enforce message signing in the node's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'.	

No.	Finding	Affected IP(s) / Status	Impact	Recommendations	Management Response
Risk rating: Medium Risk					
GBKL.TA.IIOT.2	**Multiple Vulnerabilities in Monitoring Protocols** **Executive Summary:** During the assessment, we noted that monitoring protocols **Technical Summary:** Technical Summary:During the assessment, we noted that the community name of the remote SNMP server can be guessed. It is possible to obtain the default community name of the remote SNMP server.	**OPEN** › 10.10.10.5:161 › 10.0.0.1:161	**Business Impact:** An attacker could obtain information about the host such as its operating system type and exact version, its hostname, and the list of services it is running. With these information attacker can plan the further attacks by using targeted exploits for the vulnerabilities associated to the targets. **Technical Impact:** This open port could allow attacker to obtain the default community names of the SNMP server. It is, therefore, attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system. (If the default community allows such modifications).	› Disable the SNMP service on the remote node if you do not use it. › Filter incoming UDP packets going to this port › Change the default community string.	

Evidence Finding

<table>
<tr><th>Reference No.</th><th>Evidence</th></tr>
<tr><td>

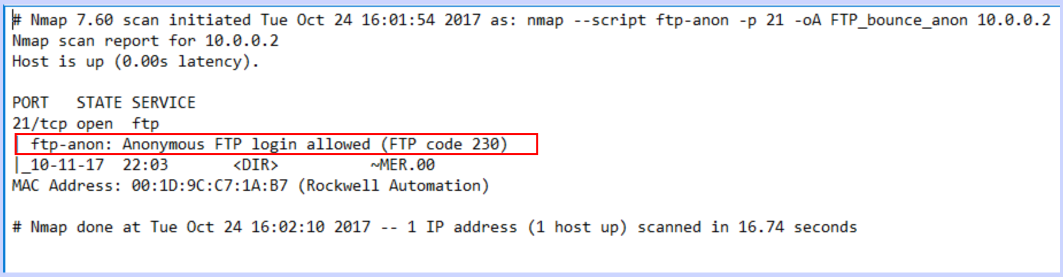
GBKL.TA.IIOT.1

</td><td>

Anonymous File Upload Enabled

(Anonymous FTP Enabled)

The screenshot below shows that the remote FTP node allows anonymous logins.



```
# Nmap 7.60 scan initiated Tue Oct 24 16:01:54 2017 as: nmap --script ftp-anon -p 21 -oA FTP_bounce_anon 10.0.0.2
Nmap scan report for 10.0.0.2
Host is up (0.00s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_10-11-17  22:03       <DIR>          ~MER.00
MAC Address: 00:1D:9C:C7:1A:B7 (Rockwell Automation)

# Nmap done at Tue Oct 24 16:02:10 2017 -- 1 IP address (1 host up) scanned in 16.74 seconds
```

</td></tr>
<tr><td>

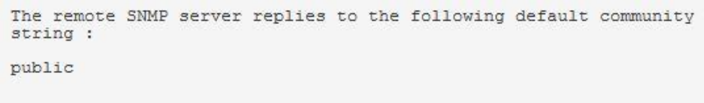
GBKL.TA.IIOT.2

</td><td>

Multiple Vulnerabilities in Monitoring Protocols

(SNMP Agent Default Community Name (public))

The screenshot below shows that the node is using the default SNMP community string (public).



```
The remote SNMP server replies to the following default community
string :

public
```

</td></tr>
<tr><td>

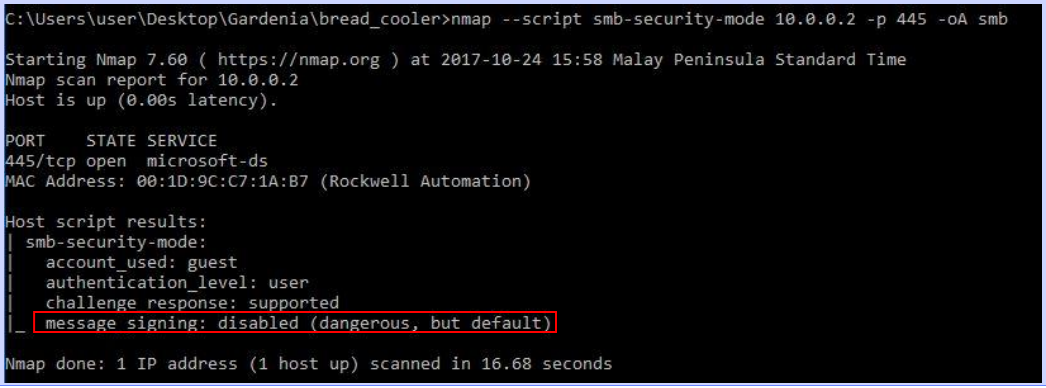
GBKL.TA.IIOT.3

</td><td>

Message Signing Disabled

(SMB Signing Disabled)

The screenshot below shows that the SMB signing is disabled.



```
C:\Users\user\Desktop\Gardenia\bread_cooler>nmap --script smb-security-mode 10.0.0.2 -p 445 -oA smb

Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-24 15:58 Malay Peninsula Standard Time
Nmap scan report for 10.0.0.2
Host is up (0.00s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:1D:9C:C7:1A:B7 (Rockwell Automation)

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

Nmap done: 1 IP address (1 host up) scanned in 16.68 seconds
```

</td></tr>
</table>

About Infopercept - Infopercept's vision and core values revolve around making organizations more secure through the core values of Honesty, Transparency and Knowledge, so as to enable them to make better informed decisions about their security practices & goals. With our synergistic vision to combine technical expertise and professional experience, we aim to further establish our place as a one stop shop for our clients and partners' cybersecurity and accreditation needs.

Imprint
© Infopercept Consulting Pvt. Ltd.

Created Date
Oct 2023

Contact Detail
sos@infopercept.com
www.infopercept.com/sample-report