Security Team Vulnerability Assessment Report

Platform Scanned

Table of Contents

Introduction

On May 3, 2022, the Security Team performed a vulnerability assessment on the scanned devices for the new platform. The second platform was not scanned due to the excessive number of vulnerabilities found combined with the less than recommended operational and security configurations presented by each system. The Security Team did not perform the availability testing due to concerns about possibly corrupting data and/or the systems. This testing will be performed after the systems are reconfigured. The Security Team will continue to assess the systems over the next several weeks. This report will lay out how the systems were assessed, the high level findings, the Security Team's recommendations, and the next steps necessary to continue the integration of the new platform into company's network.

The company does understand these devices will be in a very controlled environment with layers of security around them, but these devices will need to be accessed from other company networks which expands the attack surface. Also, there is the potential that these devices will become CIP designated assets which will require all the findings be addressed.

Note: One of the platform devices was in a failed state and could not be assessed.

Vulnerability Assessment Process

In our examination of the systems, we used a wide range of tools and tests and crawled each host. In our first test, we used an automated discovery tool to scan all the alive hosts on the network. After results came back, we started an automated vulnerability scan on each host. This Vulnerability scan hosts a catalog of the latest vulnerabilities known to be exploited in the wild, and can recognize the OS for a more comparable baseline. After the first vulnerability scan, we then run another type of scan from a different vendor. After these results come in, we compare between the two to find what relevant information there is and compare vulnerabilities.

After the scans, we take a "hardened machine approach" and look at the configuration's we use at the company when building a system we plan to introduce into our network and compare them to what the vendor (you) have sent us. From here, we moved to what we see among the network of the devices. For this part we review local firewall traffic both inbound and outbound along with ports that are active and passing traffic. Additionally we double down on identifying traffic with other traffic analyzer tools.

Findings

Note: The detailed report is over 7,000 pages in length.

Network Configuration

1. Unnecessary network services are running.

OS Licensing

1. The Windows Server OS was not licensed on any of the four Human-Machine Interface (HMI) systems.
2. The team was not able to verify the licensing on the non-Windows platforms.

Patching

1. The Windows Server OS was last patched on 04/12/2019. These machines are three years behind in patching which correlated into over 2,000 vulnerabilities found on each one.
2. Of the over 2,000 discovered vulnerabilities per HMI, 37 have automated exploits available via open-source tools.
3. The team was not able to verify the patch levels of the non-Windows platforms, but the failed device showed an error message of waiting for an upgrade.

Password Policies

1. On the Windows Server OS, the password policies were all modified to their lowest settings.
   a. Minimum Password Length = 0 => No password length requirement
   b. All account passwords are set to never expire.
   c. Account Lockout = 0 => Accounts do not lockout after a set number of failed attempts.
2. These are not the defaults provided by Microsoft.

Installed Applications

1. On the Windows Server OS, Google Chrome was installed and has not been patched.
   a. These systems were also trying to reach 8.8.8.8 (Google) on the internet.
2. All systems have vulnerable web servers running.
   a. Several web servers have Cross Site Request Forgery vulnerabilities.
   b. All web servers have TLS encryption vulnerabilities.
3. Several systems, including the Windows Server systems, have accessible databases (MongoDB, MSSQL or PostgreSQL) running.
4. MongoDB is installed on one system only and is not patched.
5. Some non-Windows systems have vulnerable OpenSSL running.
6. The Microsoft Security Baseline for Server 2019 is not installed.

Users

1. One new user was created and has administrator level privileges.
2. The Administrator account is not renamed.
3. Common usernames are being used for administrator level accounts.
4. Current passwords are not very strong.

Remote Desktop Configuration (RDP)

1. RDP is enabled with the Microsoft default configuration.
   a. This configuration is not secure.

Services

1. Several services that are not needed are either running or available to run.
2. HTTP is available, and not just on port 80, on most systems.
3. HTTPS is available on most systems.
4. NTP is configured and using an internet time source.

Anti-Virus

1. No anti-virus platform was enabled.
2. Microsoft Defender should be the minimum.

Recommendations

From the findings above, the Security Team cannot recommend this platform be allowed on the company network or in the production environment. These systems are insecure and unreliable due to the issues stated above. The Security Team proposes the following recommendations be completed before the project can continue:

1. All the software platforms need to be properly licensed.
2. All systems need to be patched to the latest patch level for all applications and operating systems.
3. The new user account with administrator privileges needs to be tested under a less privileged account level.
4. Implement new usernames for the administrator level accounts.
5. Implement new and stronger passwords for all accounts.
6. Google Chrome needs to be uninstalled or at a minimum patched.
7. RDP needs to be properly configured.
8. All systems need to be hardened which would address most of the other issues.
    a. The company has a hardening process that is used in our control environments and, if applied, this process will address most of the remaining findings.

These recommendations do not come without concerns, such as will the patching “break” the functionality of the applications, but, in their current state, these systems will put all the systems in the production environment at a higher risk of attack and/or failure.

Next Steps

Our next step is addressing and taking action of our findings. We want mitigate all vulnerabilities and harden each system, before it reaches production specifically. Below is our course of action we would like to take:

1. Contact vendor addressing the above recommendations.
2. Identify and work with the vendor on the necessary ports for each system to fully function.
3. At the result of obtaining that, we would like to drop all other ports to underline the risk of having not functional ones open.
4. Discuss the applications that came preinstalled on both of the HMI boxes and determine the need for each one and rid of the others.
5. Discuss database needs and access to other systems, rid of the “Open” concept.
6. Finally, we noticed many users are local administrators on the workstations, we would like to narrow that down to one or two users if possible, this implements the least privilege standard the company has adopted.

Meeting with the vendor addressing these questions and concerns seems in our best interest. The sooner we can meet and consult with, the earlier we can get to work patching all these systems.