# Security Assessment and Findings Report

## Business Confidential

*Date: January 9th, 2021*

This page is intentionally left blank

# Table of Contents

# Confidentiality Statement

Due to the sensitive nature of the following assessment, the information provided is protected under the DHS' Protected Critical Infrastructure Information (PCII) Program. The following document contains proprietary and confidential information designated solely to the associated parties and is the exclusive property of Next Generation Power, Electric, and Water (NGPEW) in partnership with [redacted] Permission to access, redistribute, duplicate or utilize this document (in part or in whole) requires the mutual consent of NGPEW and Team [redacted] in accordance with local and federal law.

Team [redacted] may be required to share this document with external auditors under a non-disclosure agreement in accordance with security compliance requirements.

## Disclaimer

The scope of the following security audit performed by Team [redacted] is limited to the allotted 17-hour time period as defined by the client. Thus, findings presented in the report may not fully encompass all potential vulnerabilities on the network. The following reports include only findings encountered during the assessment.

Team [redacted] highly recommends that a further evaluation of the NGPEW network is performed to ensure the confidentiality, integrity, and accessibility of all its resources. Team [redacted] recommends that external audits be conducted annually to verify that security and regulatory controls are adhered to once fully implemented by the organization.

# Scope and Limitations

### Targets of NGPEW

In-scope NGPEW network ranges as defined by the client:
`10.0.1.0/24`
`10.0.5.0/24`
`10.0.10.0/24`

### Timeframe

The testing of NGPEW was conducted during the following timeframes.
January 8, 2021 9:30 am EST - 6:00 pm EST
January 9, 2021 9:30 am EST - 6:00 pm EST

### Assets Included

The included assets within the assessment include, but are not limited to:
Industrial Control Systems (monitoring and control of water and power systems), Corporate Network Systems (Windows domain controllers and user workstations), Internal Ticketing and Messaging Systems, Customer Billing Systems, and Public Web Servers.

# Company and Network Overview

### Executive Summary

On January 8th and 9th, 2021, Team [redacted] conducted a security assessment of Next Generation Power, Electric, and Water (NGPEW) network resources and Industrial Control Systems. Team [redacted]'s testing techniques simulated an active attack against the NGPEW network to evaluate the

impact on the continued operation of the company. NGPEW intentionally withheld information on the network topology and included systems to best simulate a potential real-world attack. Given the nature of the critical infrastructure tested, Team [redacted] ensured that NGPEW customers would not experience any negative impact during or after the assessment. NGPEW and Team [redacted] conducted this test with the common goal of ensuring compliance with regulations including NERC/CIP as well as the continued operational safety and financial success of NGPEW.

[redacted] found six critical vulnerabilities that allow for the internal network of NGPEW to be compromised by attackers with unprivileged access to NGPEW's network. These vulnerabilities would allow an attacker to connect through a NGPEW workstation or web server, pivot through misconfigured Windows resources and attack critical infrastructure managed by NGPEW, threatening the safety and lives of NGPEW staff and customers. As it stands, NGPEW could be found liable for NERC/CIP violations that can account for fines of up to six figures daily.

Team [redacted] also found two high severity vulnerabilities on the internal network, consisting of internal database server workstation deployment misconfigurations. These misconfigurations do not have the same implications to operational safety at NGPEW but threaten account compromise for a wide range of systems and users. These findings also present regulatory risks to NGPEW.

In reporting the team also discovered five medium severity vulnerabilities. These do not have system-wide implications but could present the potential for individual user accounts to be compromised and facilitate wider-ranging attacks.

While Team [redacted] found NGPEW's layered network architecture isolating ICS infrastructure from its corporate and public-facing network to be a valuable deterrent against attacks, Team [redacted] advises implementing access controls and network segmentation as well as remediating these internal network misconfigurations to strengthen NGPEW's safety posture and regulatory compliance.

### Assessment narrative

At 9:30 am EST on Friday, January 8th, 2020 Team [redacted] began its penetration test of NGPEW's internal networks by conducting a ping scan on subnet 10.0.1.0/24. The team discovered several hosts in this scan, including four Windows workstations, a Windows server acting as an Active Directory Domain Controller, and a web server hosting the Rocket.Chat internal

communications platform. Detailed scans on these services revealed the Active Directory fully qualified domain name and host names of the domain controller and Windows workstations.

The team also attempted to discover hosts on the subnets 10.0.5.0/24, 10.0.10.0/24 but did not find any active hosts that they could reach from their position on the network. Following these scans, the team tried connection-less nmap scans to discover hosts on these subnets but did not get a response from any.

Team [redacted] attempted enumerating SMB shares on the Windows workstations and the domain controller, but could not connect without a valid set of credentials. Using a list of users compiled from publicly available resources, including NGPEW's public-facing website and an organizational chart available on GitHub, Team [redacted] validated 30 different Active Directory users. They attempted to use a technique known as AS-REP Roasting to connect to the Active Directory domain without the user's passwords, but none of the users were configured to produce a Kerberos Ticket Granting Ticket without valid login credentials. The team also attempted brute-forcing user logins on Active Directory but found that user accounts would get locked out after ten failed logon attempts.

While attempting to bypass Kerberos authentication on the domain controller, Team [redacted] also checked the server for vulnerabilities to high-risk low-effort Windows service vulnerabilities such as BlueKeep and Zer0logon. Team [redacted] found that NGPEW had patched against both vulnerabilities.

The team also attempted accessing the Rocket.Chat server without valid user or administrator logon credentials. Unlike the previous assessment, in which the team registered a user and signed in under that account, the Rocket.Chat server had disabled user registration. Team [redacted] attempted to enumerate users and administrator information from Rocket.Chat's REST API, but could not obtain sensitive information without a valid account. The team continued running scans and ran a timed brute-force password spray script on the Active Directory domain overnight.

At 9:30am EST on January 9th, Team [redacted] continued its assessment of NGPEW's network. Team [redacted] determined that SMB shares on Windows workstations were indeed available, and found that they could attempt logging in with the local Administrator account on these workstations. At 11:40am EST Team [redacted] succeeded in bruteforcing the local Administrator login credentials for

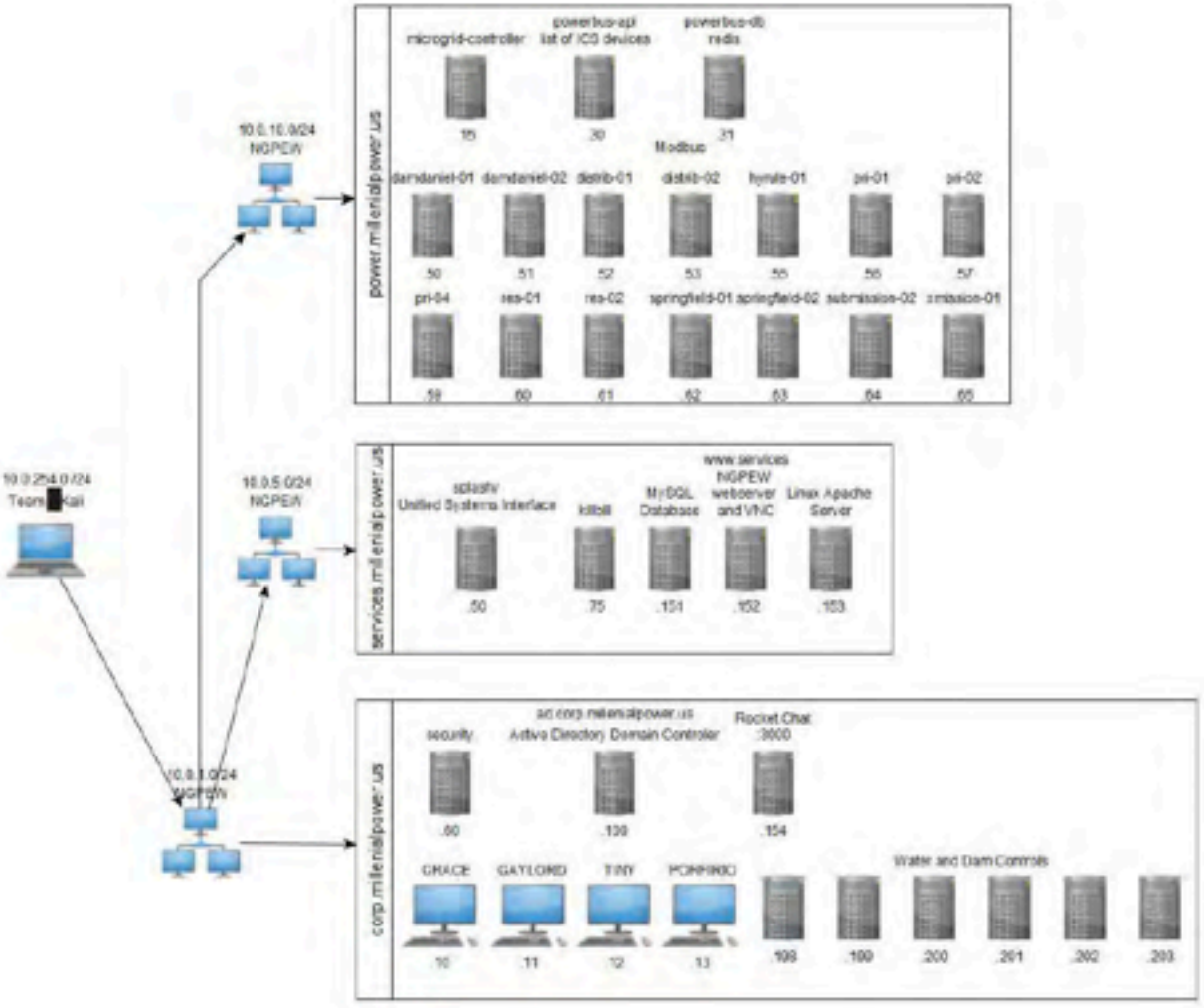
these workstations. The team installed tools on these workstations for enumerating and fingerprinting further endpoints on the network.

The team also worked to find a set of login credentials from an email on one of the workstations. Team [redacted] opened an unauthenticated VNC connection to the HMI station splashy.services.millenialpower.us from one of the workstations. The team found that splashy communicated directly with PLCs on subnet `10.0.10.0/24` (`power.millenialpower.us`). Team [redacted] was also able to reach Modbus/TCP interfaces on this subnet from the workstations it had accessed on the corporate subnet `10.0.1.0/24`.

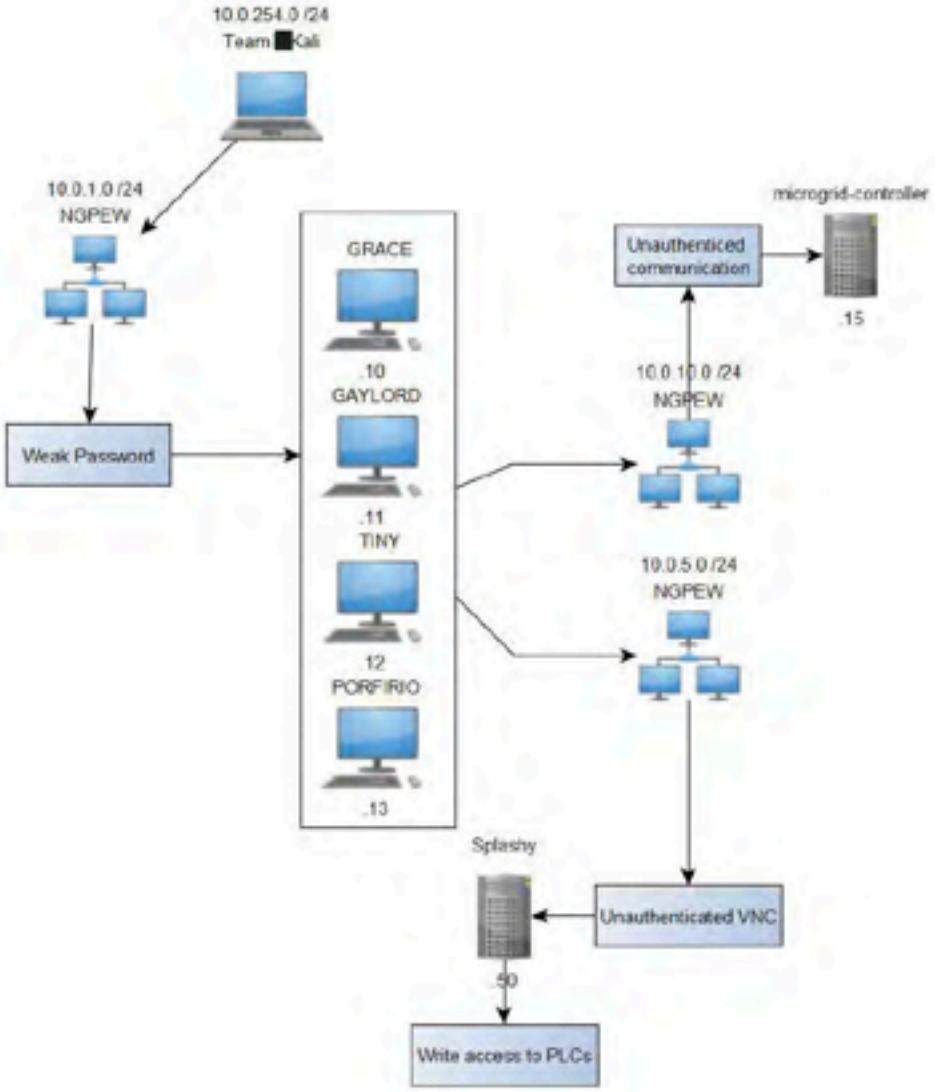
At 1:42pm EST NGPEW's IT staff provided access to an additional Linux host on the network from which Team [redacted] could conduct further testing. Team [redacted] ran continued scans on devices on NGPEW's network, discovering an IIS web server hosting a copy of NGPEW's public-facing website. This server was running IIS 4.0 on Windows NT 4.0 SP3, an operating system from 1997. The team identified several vulnerabilities to attacks allowing remote code execution (RCE) on the server and began testing if the server was susceptible. At 4:30pm EST Team [redacted] lost access to ports 80 and 443 on this server.

At 5:00pm EST, Team [redacted] made a final cataloguing of findings and began removing tools and evidence of intrusion from NGPEW assets. Team [redacted] concluded its hands-on assessment at 5:59pm EST.

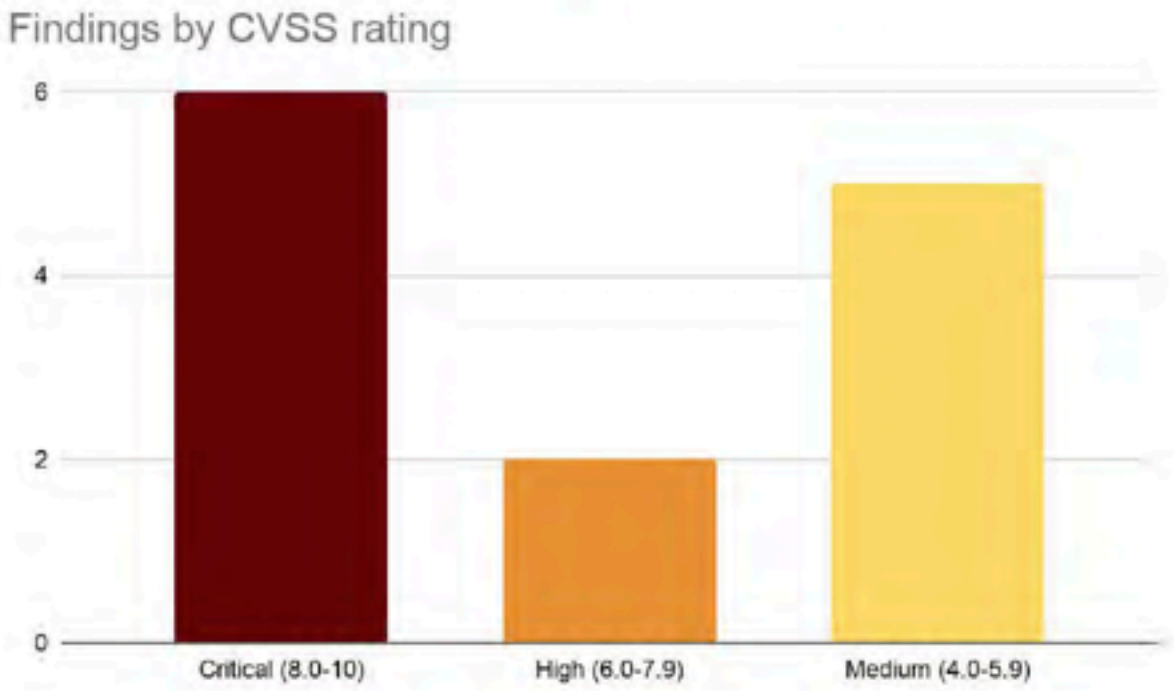
# Network Map


power.millenialpower.us
microgrid-controller
powerbus-api
list of ICS devices
powerbus-db
redis
.10
.20
.21
Modbus
darndaniel-01
darndaniel-02
distrib-01
distrib-02
hynate-01
pri-01
pri-02
.50
.51
.52
.53
.55
.56
.57
pri-04
res-01
res-02
springfield-01
springfield-02
submission-02
submission-01
.59
.60
.61
.62
.63
.64
.65
10.0.10.0/24
NGPEW
services.millenialpower.us
splashtv
Unified Systems Interface
killbill
MySQL
Database
www.services
NGPEW
webserver
and VNC
Linux Apache
Server
.50
.75
.151
.152
.153
10.0.5.0/24
NGPEW
10.0.254.0/24
Team Kali
corp.millenialpower.us
security
.50
ad.corp.millenialpower.us
Active Directory Domain Controller
.100
Rocket.Chat
:3000
.154
GRACE
.10
GAYLORD
.11
TINY
.12
PENNINGTON
.13
Water and Dam Controls
.199
.199
.200
.201
.202
.203

# “Kill Chain”



# Vulnerability Summary



## NERC/CIP Compliance Risks


## Findings by Type

# Assessment Overview

## Prior Engagement Improvements

### Network Segmentation/Purdue Model Implementation

An additional subnet, `10.0.5.0/24` was created and deployed into the production environment. The web server and HMI were relocated onto it, offering more protection for these sensitive systems. This conforms to the "Purdue Model" of ICS networks, a layered approach isolating corporate/IT assets from critical infrastructure components.

### Hardened Network

Of the three subnets in scope, only one, `10.0.1.0/24` was immediately discoverable with ping scans. It is especially good that the PLC subnet, `10.0.10.0/24`, was not immediately discoverable.

### Domain Controller Password Lockout

A lockout policy was put in place on the Domain Controller of the domain corp.millenialpower.us on the `10.0.1.0/24` subnet. The policy will lock out an account for five minutes after making ten unsuccessful login attempts.

### Domain Controller Patch Policy

The Domain Controller at `10.0.1.100` is patched beyond the 2019 CVE Bluekeep and the Zer0logon vulnerability. These recent patches are important because the Domain Controller is running 2012 R2, an older OS that while it has ended mainstream support as of January 9, 2018, it has extended support until January 10, 2023. Team [redacted] recommends upgrading the Domain Controller.

### Corporate Chat Authorized Access Only

The internal Rocket.Chat, located at `10.0.1.154:3000`, no longer allows new user registration from its homepage. Presumably the administrator creates new accounts when needed. This measure makes it more difficult for attackers to eavesdrop on sensitive information.

### Public Company Hierarchy Topology (Github)

The public company hierarchy topology chart is no longer easily visible on GitHub. However, it is still recoverable through the repository history, as detailed in finding M-03.

### Redis Database Password Changed

The Redis database password on `10.0.10.31` was changed. Team [redacted] was unable to brute force the credentials.

### Removal of VNC Server

The VNC server that was running on one of the workstations, `10.0.1.12`, was no longer present and Remote Desktop was enabled in its place. This VNC server also had a local file inclusion exploit which was no longer present.

### Removal of Mantis Bug Tracker

The Mantis Bug Tracker had multiple CVEs present that in succession allowed changing the administrator password and remote code execution. It was also recommended looking into alternatives due to weak password hashing algorithms. Team [redacted] was unable to find the Mantis Bug Tracker software on the corporate network during the latest engagement. The server that we assume used to have Mantis installed, did not respond with anything but a blank directory listing of the root web directory.

# Critical Findings

## Insecure Network Topology

| Finding ID | Severity | Affected Hosts | NERC/CIP Regulation | CVE |
|---|---|---|---|---|
| C-01 | 9.9 (Critical) | 10.0.1.0/24<br>10.0.5.0/24<br>10.0.10.0/24 | CIP 005-5<br>CIP 007-6 | N/A |

### Description

Team [redacted] found insufficient controls between NGPEW's internal subnets, `corp.millenialpower.us`, `services.millenialpower.us`, and `power.millenialpower.us`. Users with access to workstations on the corporate/IT network had unrestricted access to ICS devices including PLCs on the power subnet. This violates NERC/CIP regulation CIP 005-05, requiring electronic security perimeters (ESPs) between networks.

### Impact

A user on the corporate/IT network could access sensitive ICS devices within the network. This implies an attacker who is able to compromise a corporate device can easily escalate their attack to critical infrastructure components controlled by NGPEW. These components are not isolated from the corporate/IT network by any kind of firewall and no Intrusion Prevention System (IPS) is in place to prevent attackers from pivoting between different segments of the network. Legitimate changes from the IT

staff at NGPEW can potentially have adverse effects on ICS equipment, causing potential safety issues from within.

A network topology without segmentation violates CIP 005-05, section (1.1), requiring assets reside within an ESP. CIP 005-05 also requires access controls per section (1.3) and application layer firewalls per section (1.6). Remote access should be conducted and encrypted through intermediary systems per CIP 005-05 sections (2.1) and (2.2)

**Steps to Reproduce**

Upon accessing a Windows workstation on the corp.millenialpower.us subnet (`10.0.1.0/24`) (as covered in finding C-03), Team [redacted] could scan PLC devices on the power.millenialpower.us (`10.0.5.0/24`) subnet and HMI/SCADA devices on services.millenialpower.us (`10.0.10.0/24`). The team was able to test access to these devices by installing nmap on the Windows workstation hosts and running scans of each subnet. Team [redacted] has provided samples from scan results below:

```
Nmap scan report for splashy.services.millenialpower.us (10.0.5.50)
Host is up, received echo-reply ttl 128 (0.013s latency).
Scanned at 2021-01-09 17:36:34 Coordinated Universal Time for 2846s
Not shown: 65530 filtered ports
Reason: 65530 no-responses
PORT     STATE SERVICE       REASON          VERSION
135/tcp  open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
139/tcp  open  netbios-ssn   syn-ack ttl 128 Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  syn-ack ttl 128 Microsoft Windows Server 2008 R2 - 2012
microsoft-ds
3389/tcp open  ms-wbt-server syn-ack ttl 128 Microsoft Terminal Services
| ssl-cert: Subject: commonName=splashy
| Issuer: commonName=splashy

# Nmap 7.80 scan initiated Sat Jan  9 22:36:29 2021 as: nmap -Pn -p502 -T1 -oN
modbus-scan_50-57.txt 10.0.10.50-57
Nmap scan report for ip-10-0-10-50.ec2.internal (10.0.10.50)
Host is up (0.0011s latency).
```

```
PORT    STATE SERVICE
502/tcp open  mbap
Nmap scan report for ip-10-0-10-51.ec2.internal (10.0.10.51)
Host is up (0.0012s latency).

PORT    STATE SERVICE
502/tcp open  mbap

Nmap scan report for ip-10-0-10-52.ec2.internal (10.0.10.52)
Host is up (0.0012s latency).

PORT    STATE SERVICE
502/tcp open  mbap
```

### Finding Comments

Though the team's initial hosts on the network could not reach devices on the `power.corp.millenialpower.us` or `services.corp.millenialpower.us` subnets, NGPEW failed to implement these restrictions to other devices on the `corp.millenialpower.us` subnet.

### Recommendations

Implement network segmentation. Limit access between hosts on different subnets. Many ICS networks encompassing both IT and OT environments implement network security and security by implementing a tiered "Purdue Model" network.


Network segmentation according to the Purdue model is applicable to the several ICS environments, including manufacturing (as pictured in the attached diagram sourced from https://www.controldesign.com) as well as power distribution. Team [redacted] advises placing SCADA devices such as the HMI computer on

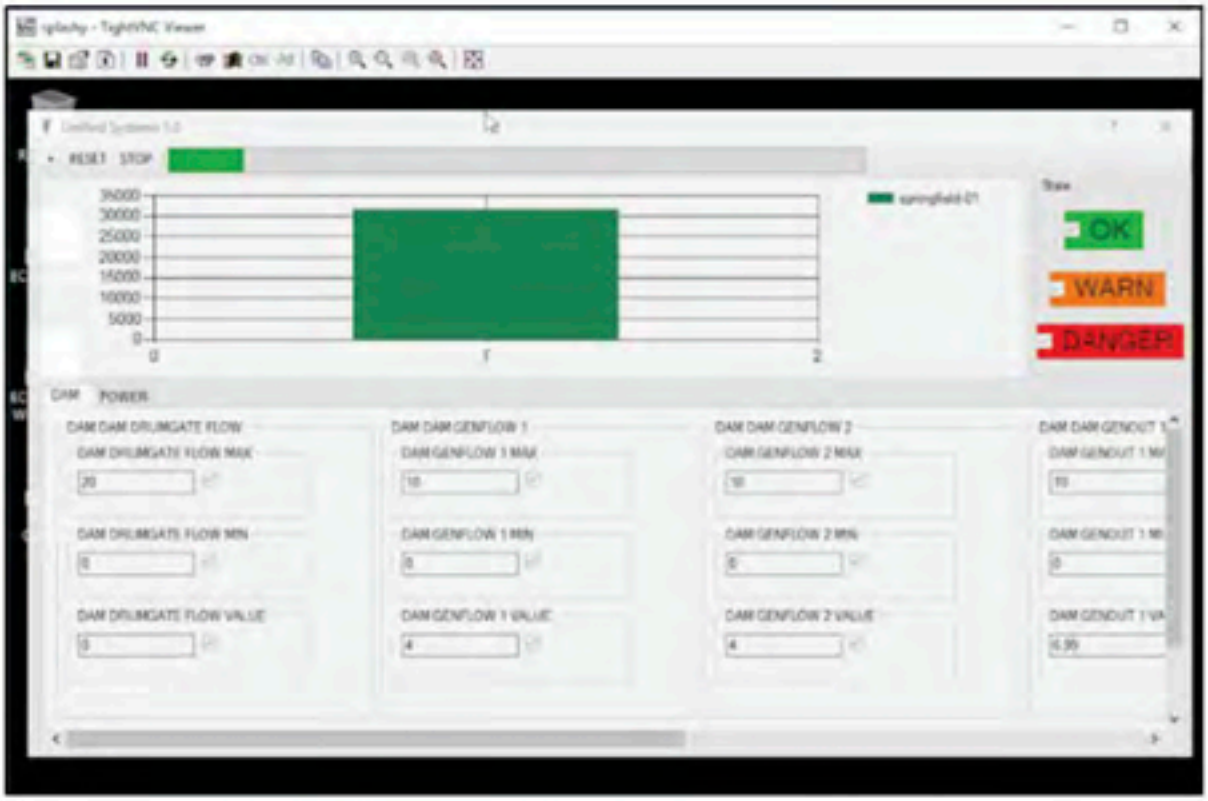
10.0.5.50 on a separate control network, between enterprise/services networks and process control networks.

## Unauthenticated VNC Connection

| Finding ID | Severity | Affected Hosts | NERC/CIP Regulation | CVE |
|---|---|---|---|---|
| C-02 | 9.6 (Critical) | 10.0.5.50 | CIP 007-6 | N/A |

### Description

Team [redacted] discovered that there was no authentication set up for VNC connections on 10.0.5.50, port 5900. Team [redacted] was able to connect with TightVNC and identify it as a Windows 2016 Datacenter. This server had a hostname of "SPLASHY". Team [redacted] had access to an administrator account and to software called Unified Systems 1.0. This software could change various settings for remote power generation systems.




### Impact

Unified Systems 1.0 allows the user to read real-time values of the systems and possibly alter these values which could potentially lead to catastrophic disaster.

### Steps to Reproduce

Through Nmap, the team discovered the VNC port 5900 open on server `10.0.5.50` which does not require authentication. Using the TightVNC client the team connected to the VNC.

```
5900/tcp open  vnc           syn-ack ttl 128 VNC (protocol 3.8)
| vnc-info:
|   Protocol version: 3.8
|   Security types:
|     None (1)
|     Tight (16)
|   Tight auth subtypes:
|     None
|_  WARNING: Server does not require authentication
```

### Finding Comments

An open VNC connection without authentication leads to the exposure of all information stored within the server. Enumeration of the local file system yields sensitive data.

### Recommendations

Set up system authentication with VNC or use another protocol requiring authentication.

### NERC CIP Penalty Range

$10,000 - $335,000

## Weak Local Administrator Password

| Finding ID | Severity | Affected Hosts | NERC/CIP Regulation | CVE |
|---|---|---|---|---|
| C-03 | 9.6 (Critical) | 10.0.1.10<br>10.0.1.11<br>10.0.1.12<br>10.0.1.13 | CIP 005-5<br>CIP 007-6 | N/A |

### Description

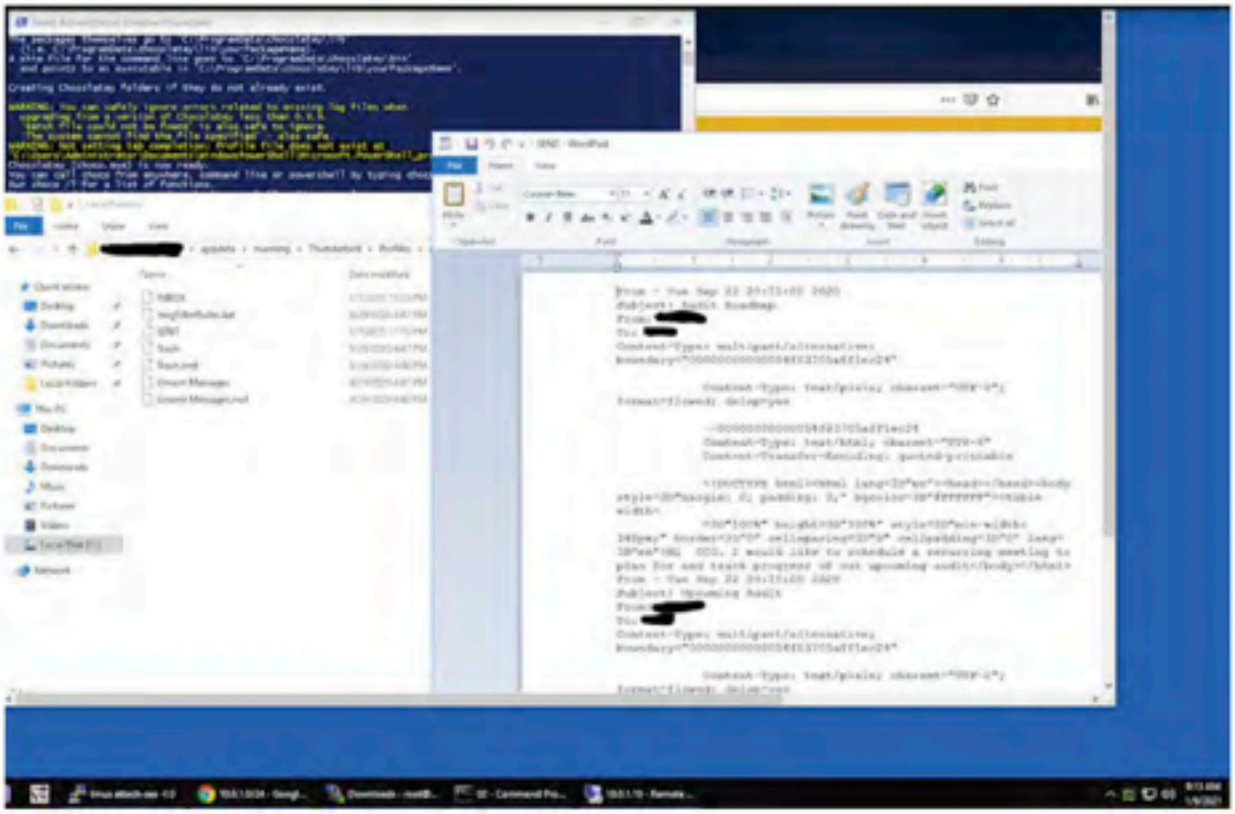
Team [redacted] was able to brute force login credentials for the local administrator on Windows workstation hosts `10.0.1.10`, `10.0.1.11`, `10.0.1.12`, and `10.0.13`. Each host had one of two nearly identical passwords, which the team guessed using a brief script they created within minutes. Weak controls on systems connected to Bulk Electric Systems (BES) violate NERC/CIP regulations CIP 005-05 and CIP 007-6.

### Impact

A local administrator on a Windows workstation has privileges to create and delete local users and to access the entire filesystem of the computer. The administrator account can read, modify, and exfiltrate data from any other user account on the system. In the case of these workstations, Team [redacted] used the local administrator account to view the contents of emails saved to domain user profiles on the system.

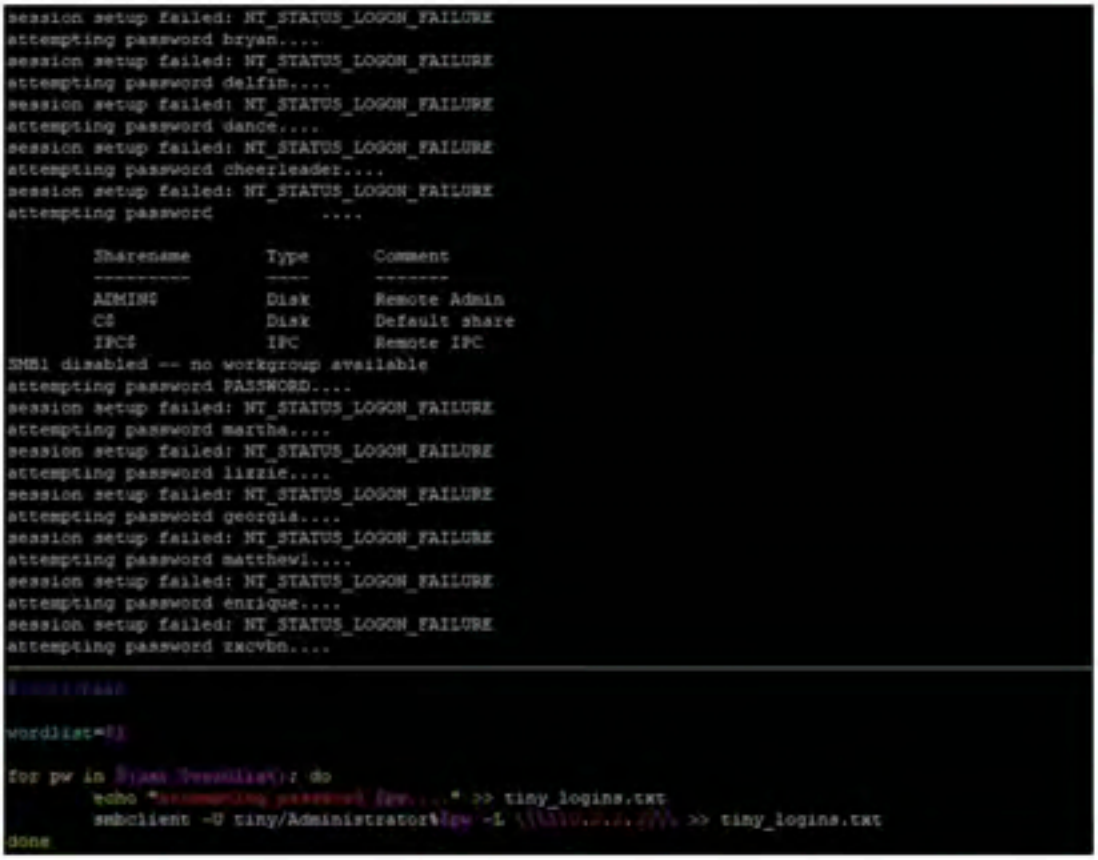
The password to this system did not adhere to CIP 007-6 section (5.5), requiring a password consist of at least 3 different types of characters (uppercase, lowercase, numeric, and non-alphanumeric characters). CIP 007-6 section (5.7) requires generating alerts or account blocks for repeated unsuccessful login attempts, which was not enforced on these local administrator accounts.

Team ▉ leveraged the local administrator account to copy additional stored credentials on the Windows workstations and connect to other servers and ICS components on the network (see findings C-01, C-04, and M-01).



### Steps to Reproduce

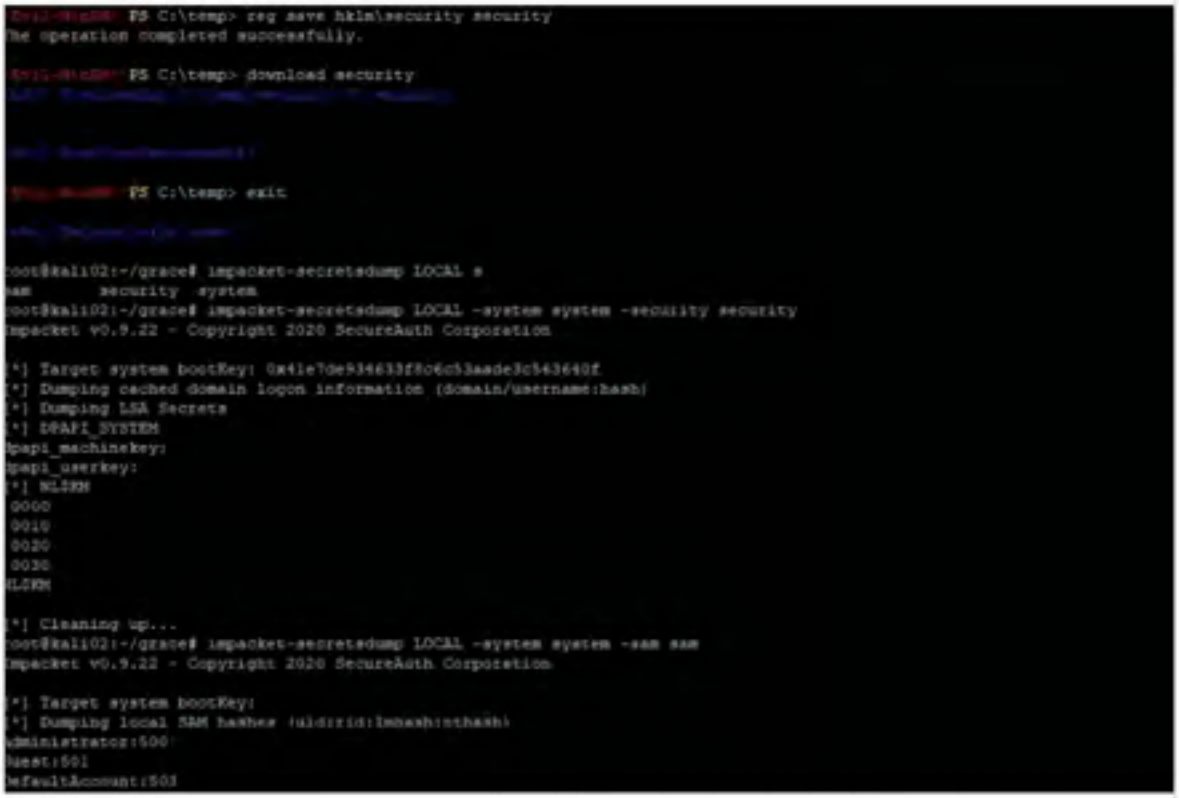
Team ▉ discovered that a local account on the workstation at `10.0.1.11` was able to access an SMB share from the network. The team then created a script to iterate through different passwords and attempt logging in to the SMB share.




Upon finding a password that could log in to the SMB share, the team used the account credentials to log in over RDP.

From the local administrator account Team ▌ demonstrated the capability to dump further credentials and secured assets on the machine. As a local administrator, Team ▌ was able to copy encrypted credentials stored in the Windows registry hive `HKEY_LOCAL_MACHINE\SECURITY` and `HKEY_LOCAL_MACHINE\SAM`, as well as the decryption keys stored in `HKEY_LOCAL_MACHINE\SYSTEM`.

Using the `impacket-secretsdump` tool, Team [redacted] pulled hashes of local users on the machine. `impacket-secretsdump` would also have been able to pull domain user credentials from these registry entries if these workstations were connected to the domain (see finding M-04).




### Recommendations

Implement a more complex logon password for local administrator accounts. NERC/CIP regulation CIP 005-05 requires passwords of 8 characters or more. Team [redacted] advises using passwords greater than 14 characters at least, and ensuring that the password is not already included in the sort of list of compromised passwords that was used to brute force this login.

## Reuse of Local Administrator Password

| Finding ID | Severity | Affected Hosts | NERC/CIP Regulation | CVE |
|---|---|---|---|---|
| C-03a | 9.6 (Critical) | 10.0.1.10<br>10.0.1.11<br>10.0.1.12<br>10.0.1.13 | CIP 005-5<br>CIP 007-6 | N/A |

### Description

Team [redacted] discovered credential recycling in place on the local administrator accounts of hosts `10.0.1.10`, `10.0.1.11`, `10.0.1.12`, and `10.0.1.13`. Using the same password (or after slightly modifying the password) the team quickly pivoted between four different Windows hosts.

### Impact

The reuse of administrator passwords risks violation of NERC/CIP regulation CIP 005-05, enforcing access control on networks affecting BES.

Reuse of local administrator account credentials also amplifies the threat that an attacker presents after compromising just one business system. Rather than isolating the breach to one machine, the attacker can reuse these credentials to pivot through the network, gather further information to exfiltrate or leverage in further attacks, and access more connected systems.

### Steps to Reproduce

The local administrator accounts on workstations `10.0.1.10` and `10.0.1.13` reused the same password that Team [redacted] found as a local administrator credential on `10.0.1.11`. Team [redacted] changed one character in this password in order to access the local administrator account on `10.0.1.13`.

The team logged into these accounts using Remote Desktop as well as the `wsman` Powershell client `evil-winrm`.

### Recommendations

Managing local administrator accounts presents a challenge to IT organizations, but it is important to enforce secure account management in order to limit the impact of an account breach on a network. Team [redacted] recommends using a Privileged Access Management or Password Management tool to allow local administrators on each machine to have a different set of credentials. The team also strongly recommends the use of MFA on administrator accounts wherever possible to comply with NERC/CIP regulations and limit the ability for attackers to access highly privileged accounts.

## PLCs/Modbus Ports Available from Corporate Network

| Finding ID | Severity | Affected Hosts | NERC/CIP Regulation | CVE |
|---|---|---|---|---|
| C-04 | 9.1 (Critical) | 10.0.10.50-65 | CIP 005-5 | N/A |

### Description

Team [redacted] discovered that various addresses on the `10.0.10.0/24` subnet had port 502 open and running the modbus protocol. The modbus protocol allows reading and writing values to programmable logic controllers.

### Impact

This exposure represents violations of NERC/CIP regulations CIP 005-5 (section 2.1), advising remote access to high impact assets through intermediate systems, as well as CIP 011-2, which advises protections for BES Cyber System Information. Any user on the corporate network has direct access to systems controlling NGPEW access, allowing them to monitor and alter PLC settings, representing a severe threat of service disruption and loss of human life.

### Steps to Reproduce

Running the scan from a machine inside the corporate network, the team discovered the open ports, [redacted] intentionally used the `-T2` flag to reduce the timing for the purpose of not damaging the sensitive PLCs.

```
$ nmap -Pn -T2 -p 502 10.0.10.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-09 22:35 UTC
Initiating Parallel DNS resolution of 256 hosts. at 22:35
Completed Parallel DNS resolution of 256 hosts. at 22:35, 0.21s elapsed
Initiating Connect Scan at 22:35
Scanning 256 hosts [1 port/host]
Discovered open port 502/tcp on 10.0.10.50
Discovered open port 502/tcp on 10.0.10.51
Discovered open port 502/tcp on 10.0.10.52
Discovered open port 502/tcp on 10.0.10.55
Discovered open port 502/tcp on 10.0.10.56
Discovered open port 502/tcp on 10.0.10.57
Discovered open port 502/tcp on 10.0.10.59
Discovered open port 502/tcp on 10.0.10.60
Discovered open port 502/tcp on 10.0.10.62
Discovered open port 502/tcp on 10.0.10.61
Discovered open port 502/tcp on 10.0.10.63
Discovered open port 502/tcp on 10.0.10.64
Discovered open port 502/tcp on 10.0.10.65
Discovered open port 502/tcp on 10.0.10.53

...

Nmap scan report for ip-10-0-10-50.ec2.internal (10.0.10.50)
Host is up, received user-set (0.0013s latency).
Scanned at 2021-01-09 22:35:07 UTC for 0s

PORT    STATE SERVICE REASON
502/tcp open  mbap    syn-ack

Nmap scan report for ip-10-0-10-51.ec2.internal (10.0.10.51)
Host is up, received user-set (0.0012s latency).
Scanned at 2021-01-09 22:35:07 UTC for 0s

PORT    STATE SERVICE REASON
502/tcp open  mbap    syn-ack

Nmap scan report for ip-10-0-10-52.ec2.internal (10.0.10.52)
```

```
Host is up, received user-set (0.0015s latency).
Scanned at 2021-01-09 22:35:07 UTC for 0s

PORT    STATE SERVICE REASON
502/tcp open  mbap    syn-ack
```

The team then used Modbus Examiner to connect and read a value from `10.0.10.65`.


## Recommendations

Modbus is a protocol without any security measures. All Modbus traffic over TCP is unencrypted, so anyone on the network can capture and replay packets used to communicate with Modbus devices. Furthermore, no authentication is required to send commands and alter registers on modbus devices. All the PLCs should be on their own subnet with a firewall with an IDS/IPS and rules in place that only allows requests from `10.0.10.15` (the machine that has the HMI web application backend), and management.

## Web Server Patch Status

| Finding ID | Severity | Affected Hosts | NERC/CIP Regulation | CVE |
|---|---|---|---|---|
| C-05 | 8.8 (Critical) | 10.0.5.152 | CIP 007-6<br>CIP 010-2 | MS02-018<br>CAN-2001-0500<br>CVE-2008-4770 |

### Description

Team [redacted] discovered the web server, www.services.millenialpower.us at `10.0.5.152` using IIS (Internet Information Services) 4.0 and running an unsupported version of Microsoft Windows NT 4.0 SP3 (released May 15, 1997). The server hosts the public website, www.NGPEW.com, and is accessible internally via RealVNC Server version 4.0 (released mid to late 2000's).
Although Team [redacted] did not gain access to the host, there are a staggering number of available vulnerabilities (such as MS02-018) for Windows NT 4.0 SP3, IIS 4.0, and RealVNC Server 4.0.

### Impact

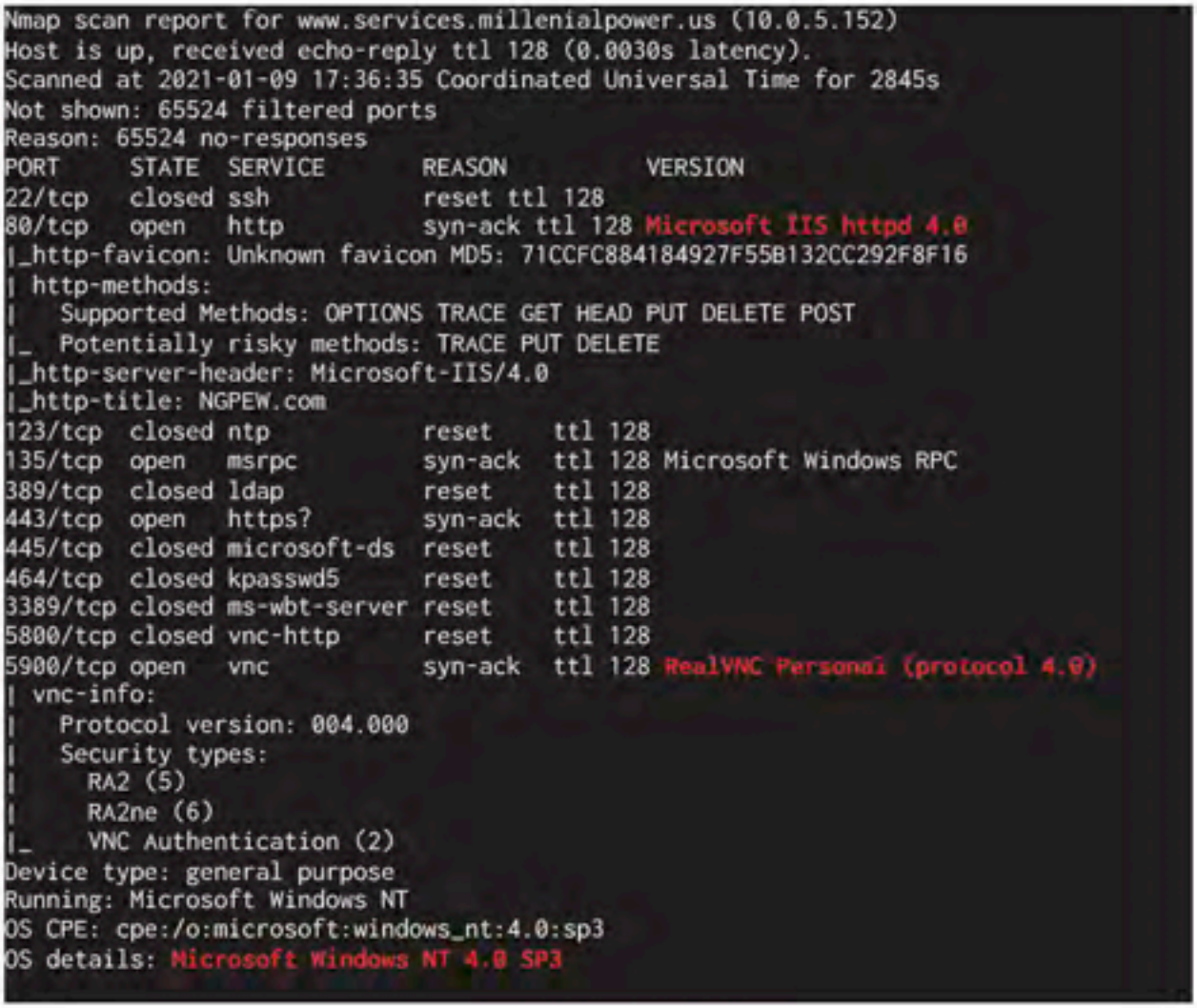
Access to this server will allow attackers to view and modify its data including the webpage which it serves. Well-known attack vectors can be utilized to take complete control over the server and all data on it impacting the public facing image of the company and disrupting client-facing interactions.

IIS 4 and IIS 5 are affected by the CA-2001-13 security vulnerability which led to the infamous Code Red (https://www.sans.org/security-resources/malwarefaq/code-red) attack.

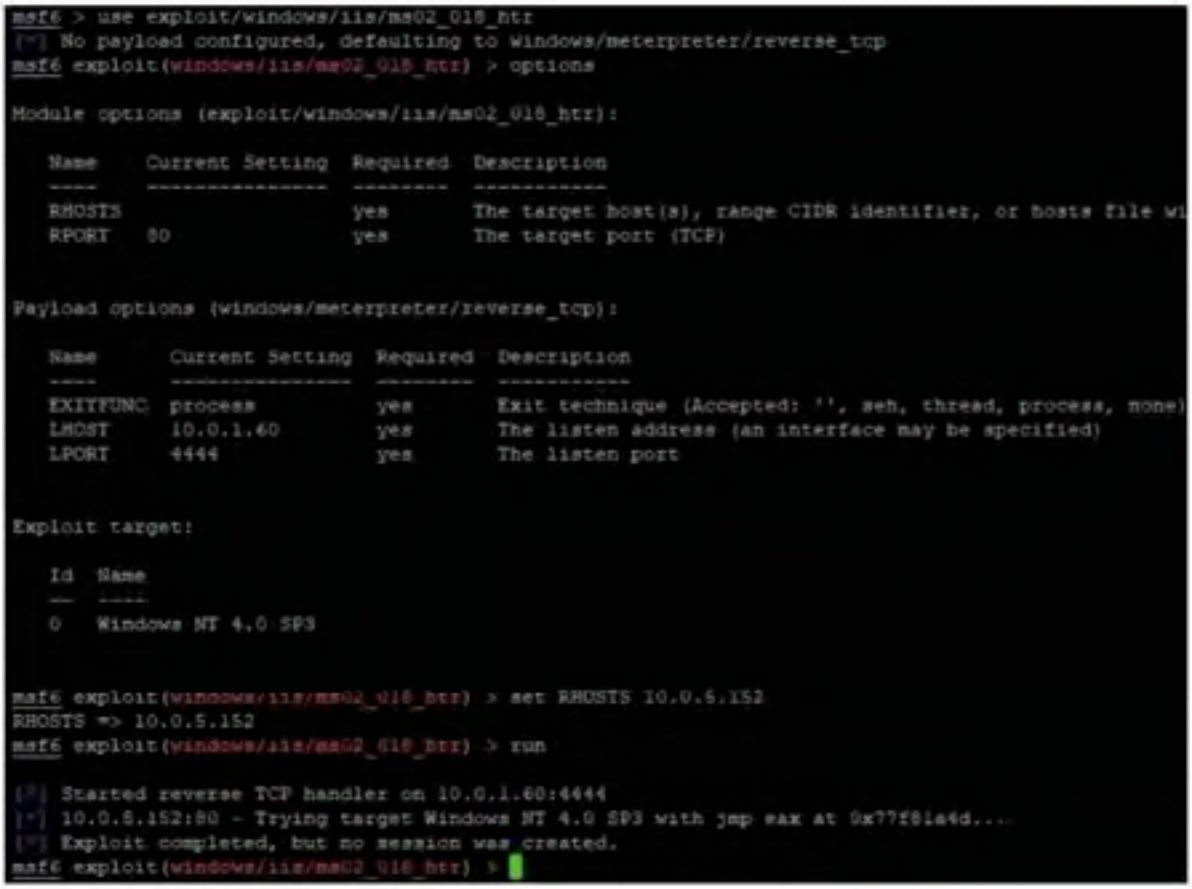
In email correspondence with NGPEW Support, it was identified that the server has been in production “for a decade” which may signal noncompliance of CIP 007-6 Section 2.2 in regards to available patches being reviewed and applied every 35 days.


### Steps to Reproduce

After getting access to workstations (finding C-03) it was possible to scan the services.millenialpower.us (`10.0.5.0/24`) subnet with Nmap.
It revealed the server `www.services.millenialpower.us` (`10.0.5.152`), its OS, and services it was running along with their versions.




After running Metasploit module `exploit/windows/iis/ms02_018_htr` ports 80 and 443 appeared as closed. Thinking this crashed the web server, Team [redacted] immediately reached out to NGPEW Director of Information Technology, Gaylord Schaefer to resolve the issue.




### Finding Comments

Using end-of-life and unsupported software introduces the potential for well-known attack vectors to be exposed to attackers. Given additional time, Team [redacted] would like to run additional tests on this server to further confirm possible vulnerabilities.

### Recommendations

According to aforementioned CIP 007-6 Section (2.2), new security patches have to be evaluated every 35 days, tested, and implemented. This server should be updated to the latest supported version available from Microsoft allowing for continued security and service patches to be applied.

# Critical Severity Findings

## HMI Web Application Backend Freely Accessible

| Finding ID | Severity | Affected Hosts | NERC/CIP Regulation | CVE |
|---|---|---|---|---|
| C-06 | 8.2 (Critical) | 10.0.10.15 | NERC/CIP 005-5 | N/A |

### Description

Team [redacted] discovered the web application backend used in combination with the human machine interface (SecureController), which is used to communicate with various PLCS, was freely accessible within the corporate network, uses unencrypted transport, and has no authentication. This allows anyone with access to a machine on the corporate network, to write values to the PLCs via a POST request to the HMI web application backend on `10.0.10.15`.

### Impact

This exposure represents violations of NERC/CIP regulations `CIP 005-5` section (2.1), advising remote access to high impact assets through intermediate systems, as well as CIP 011-2, which advises protections for BES Cyber System Information. Any user on the corporate network has indirect access to systems controlling NGPEW access, allowing them to monitor and alter PLC settings, representing a severe threat of service disruption and loss of human life.

### Steps to Reproduce

Information was discovered through a couple separate avenues. Running an nmap scan from inside the corporate network against the `10.0.10.0/24` subnet reveals a web server on `10.0.10.15` with a python web server running on port 80.

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-09 17:06 Coordinated Universal
Time
NSE: Loaded 45 scripts for scanning.
Initiating Ping Scan at 17:06
Scanning 256 hosts [4 ports/host]
Completed Ping Scan at 17:06, 13.48s elapsed (256 total hosts)
Initiating Parallel DNS resolution of 17 hosts. at 17:06
Completed Parallel DNS resolution of 17 hosts. at 17:06, 0.01s elapsed
...
Initiating SYN Stealth Scan at 17:06
Scanning 17 hosts [1000 ports/host]
Discovered open port 80/tcp on 10.0.10.15
SYN Stealth Scan Timing: About 43.59% done; ETC: 17:07 (0:00:40 remaining)
Completed SYN Stealth Scan against 10.0.10.57 in 46.06s (16 hosts left)
Completed SYN Stealth Scan against 10.0.10.59 in 46.08s (15 hosts left)
Completed SYN Stealth Scan against 10.0.10.60 in 46.20s (14 hosts left)
Completed SYN Stealth Scan against 10.0.10.64 in 46.20s (13 hosts left)
Completed SYN Stealth Scan against 10.0.10.30 in 46.25s (12 hosts left)
Completed SYN Stealth Scan against 10.0.10.31 in 46.25s (11 hosts left)
Completed SYN Stealth Scan against 10.0.10.52 in 46.28s (10 hosts left)
Completed SYN Stealth Scan against 10.0.10.50 in 46.30s (9 hosts left)
Completed SYN Stealth Scan against 10.0.10.56 in 46.31s (8 hosts left)
Completed SYN Stealth Scan against 10.0.10.63 in 46.33s (7 hosts left)
Completed SYN Stealth Scan against 10.0.10.51 in 46.39s (6 hosts left)
Completed SYN Stealth Scan against 10.0.10.53 in 46.42s (5 hosts left)
Completed SYN Stealth Scan against 10.0.10.55 in 46.42s (4 hosts left)
Completed SYN Stealth Scan against 10.0.10.61 in 46.42s (3 hosts left)
Completed SYN Stealth Scan against 10.0.10.65 in 46.42s (2 hosts left)
Completed SYN Stealth Scan against 10.0.10.15 in 46.42s (1 host left)
Completed SYN Stealth Scan at 17:07, 46.42s elapsed (17000 total ports)
Initiating Service scan at 17:07
Scanning 1 service on 17 hosts
Completed Service scan at 17:07, 6.02s elapsed (1 service on 17 hosts)
```

```
NSE: Script scanning 17 hosts.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 17:07
Completed NSE at 17:07, 0.05s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 17:07
Completed NSE at 17:07, 0.02s elapsed
Nmap scan report for microgrid-controller.power.millenialpower.us (10.0.10.15)
Host is up, received echo-reply ttl 64 (0.00020s latency).
Scanned at 2021-01-09 17:06:28 Coordinated Universal Time for 61s
Not shown: 999 filtered ports
Reason: 999 no-responses
PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 63 Werkzeug httpd 1.0.1 (Python 3.7.4)
```

Browsing to the address `http://10.0.10.15` or requesting it via curl on the command line returns a large json value representing the state of the various PLCs on the `10.0.10.0/24` subnet.

```
$ curl http://10.0.10.15
{
  "dam_elements": {
    "DAM-DRUMGATE-FLOW": {
      "max": 20,
      "min": 0,
      "status": "ok",
      "value": 12
    },
    "DAM-GENFLOW-1": {
      "max": 10,
      "min": 0,
      "status": "ok",
      "value": 7
    },

  //...

  },
  "power_elements": {
```

```
    "damdaniel-01": {
      "max": 400000,
      "min": 10000,
      "status": "ok",
      "value": 15822.20178101845
    },
    "damdaniel-02": {
      "max": 400000,
      "min": 10000,
      "status": "ok",
      "value": 46701.20560679971
    },

  //...

  },
  "ui_max": 110,
  "ui_min": 0
}
```


Decompiling the SecureController.exe found on `10.0.5.50` (SPLASHY) with dotPeek revealed code that would call a function named setState designed to send a set of values via an http POST request to the web application backend on 10.0.10.15, that ultimately would be written to the PLCs. The team refrained from testing this ourselves as we were advised by the NGPEW team that there was not a way to do it safely.

### Finding Comments

During our previous engagement we noticed that it was not possible to update values on the PLCs via the Human Machine Interface, SecureController, and/or POST requests to the web application backend. Given that it looked like the application may still have been in development at the time, the team wanted to reassess, but contacted the NGPEW team prior. [redacted] was advised that the update had been implemented, and that no tests should be run that could potentially impact the critical infrastructure.

**Recommendations**

The web application backend should only allow reading and writing sensitive information over encrypted transport, likely https in this case. The http server can still be run, but it should only redirect to https on port 443.

Sensitive operations and information should also require authentication to access. A secure login/credential system should be implemented so only authorized users are able to read and write from the PLCs. Finding an existing, known secure implementation is preferable to writing your own.

A firewall should be in place between the corporate network and the web application backend on `10.0.10.15` that only allows requests from users that need access.

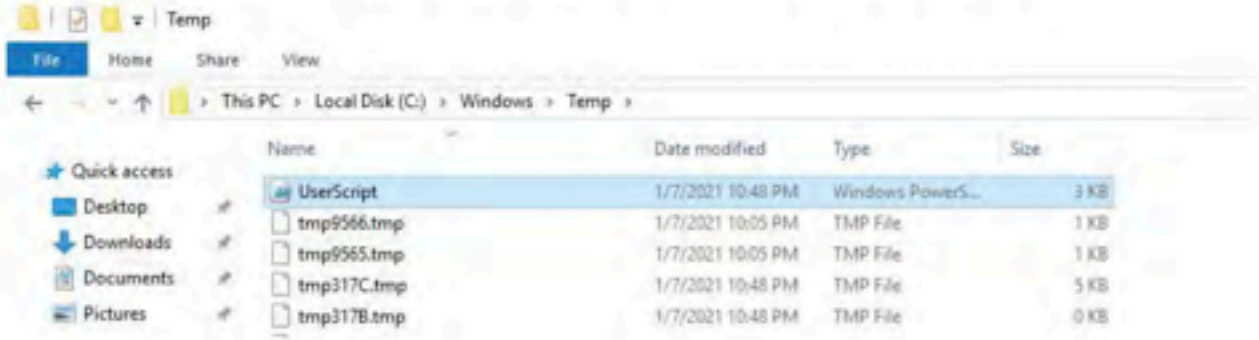
# High Severity Findings

## Insecure Setup Script - UserScript.ps1

| Finding ID | Severity | Affected Hosts | NERC/CIP Regulation | CVE |
|---|---|---|---|---|
| H-01 | 7.8 (High) | 10.0.1.10-13 | CIP 010-2<br>CIP 007-6 | N/A |

### Description

A setup script, `UserScript.ps1`, was discovered on user workstations `10.0.1.10-13` in the `C:\Windows\Temp` directory. The contents of the script include the credentials of a local administrator account exposed in cleartext. Additionally, the local Security Policy is significantly reduced by the script including disabling the local firewall.

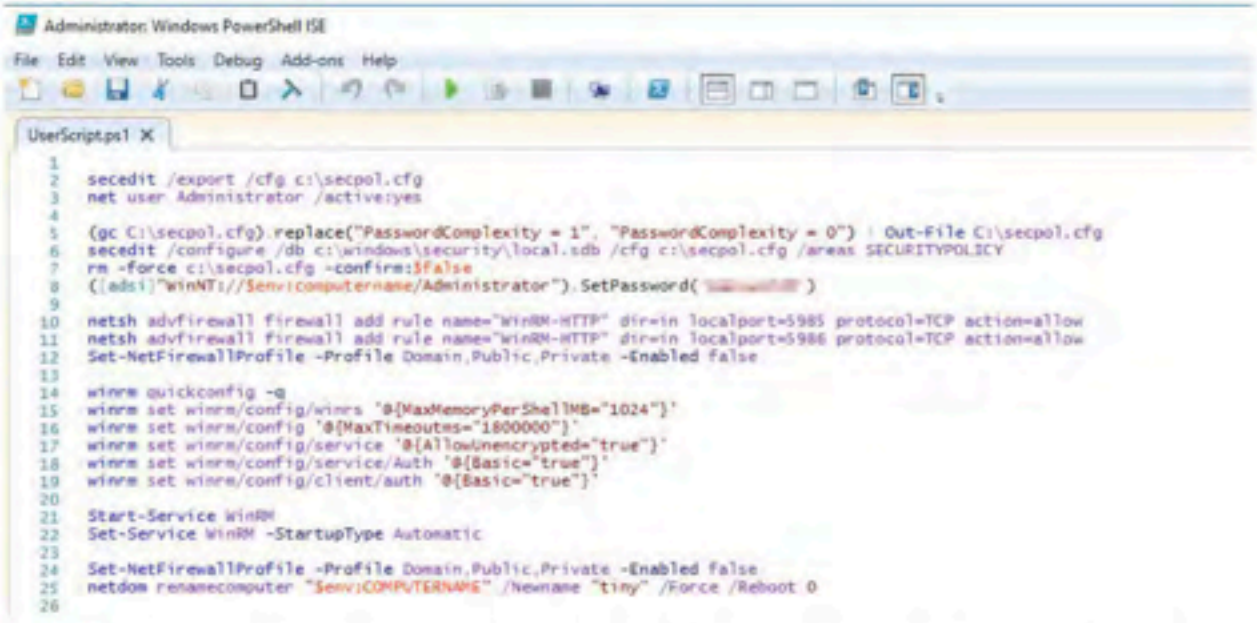


### Impact

The script was detected on the following workstation(s):

`grace (10.0.1.10), gaylord (10.0.1.11), tiny (10.0.1.12), porfilio (10.0.1.13).`

Upon execution of `UserScript.ps1`, the password complexity is reduced to the lowest possible value. In line 8, the local administrator credentials are exposed, allowing an attacker or even local user to utilize the credentials on the machine for privilege escalation.




In lines 10-12, firewall rules are added to allow TCP ports `5985` and `5986`. Additionally, Windows Firewall on all profiles is disabled. On line 17 of the following block, unencrypted WinRM traffic is set to `true`.

Exposure of the local administrator credentials is a severe violation of policy and allows for unintended, full-access to all machines on which this script is run.

### Steps to Reproduce

The script can be located for review at the `C:\Windows\Temp\UserScript.ps1` on any of the affected hosts (`10.0.1.10-13`).

### Finding Comments

View permissions are assigned to all users on the machine with access to the `C:\Windows\Temp` directory. This allows nearly all users on the machine to escalate to Administrator with little to no effort required.

### Recommendations

It is recommended that policies are pushed out via Group Policy Object instead of setup scripts. If scripts are to be used, they should be stored in a protected directory and then removed. Administrator credentials should never be exposed or retained on a machine.

## Hazardous Scripts - install.ps1

| Finding ID | Severity | Affected Hosts | NERC/CIP Regulation | CVE |
|---|---|---|---|---|
| H-01a | 7.8 (High) | 10.0.5.50 | CIP 010-2 | N/A |

### Description

After connecting to 10.0.5.50 via an unauthorized VNC connection [redacted] discovered a program running with the file name SecureController.exe that looked like custom software, as the files associated with it were a debug database and deployment/setup scripts. Among these setup scripts was a powershell script, install.ps1. This file looks to be an installation script that turns off User Account Control and the IE Enhanced Security Configuration, installs something, and then fails to turn them back on. Installing the "SecureController" looks to result in breaking access control for any machine it would be installed on. This may result in applications gaining administrator privileges without direct authorization from the administrator.

### Impact

Although the team believes that this was written by NGPEW staff, the end result is that User Account Control and IE Enhanced Security Configuration are disabled, potentially resulting in applications running with elevated privileges without the explicit authorization of the administrator, and allowing access to insecure internet and intranet websites.

### Steps to Reproduce

Team [redacted] encountered an application running after connecting to VNC that looked to give access to sensitive Dam and Power settings. After further investigation, the UI and associated files indicated an in-house solution, which commonly have security issues and/or haven't been properly tested. It also looked to be monitoring and possibly controlling ICS devices. The team used dotPeek to analyze the .Net executable, and viewed the contents of the build and deployment scripts. The following functions were found

```
function Disable-InternetExplorerESC {
    $AdminKey = "HKLM:\SOFTWARE\Microsoft\Active Setup\Installed
    Components\{A509B1A7-37EF-4b3f-8CFC-4F3A74704073}"
    $UserKey = "HKLM:\SOFTWARE\Microsoft\Active Setup\Installed
    Components\{A509B1A8-37EF-4b3f-8CFC-4F3A74704073}"
    Set-ItemProperty -Path $AdminKey -Name "IsInstalled" -Value 0 -Force
    Set-ItemProperty -Path $UserKey -Name "IsInstalled" -Value 0 -Force
    Remove-ItemProperty -Path $AdminKey -Name "IsInstalled" -Force
    Remove-ItemProperty -Path $UserKey -Name "IsInstalled" -Force
    start-process "cmd.exe" "/c C:\hmi\breakie.bat"
    Stop-Process -Name Explorer -Force
    Write-Host "IE Enhanced Security Configuration (ESC) has been disabled." -
    ForegroundColor Green

}

function Disable-UserAccessControl {
    Set-ItemProperty
    "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name
    "ConsentPromptBehaviorAdmin" -Value 00000000 -Force
    Write-Host "User Access Control (UAC) has been disabled." -ForegroundColor
     Green
}
```

### Finding Comments

This is not a new finding and was also present during our first engagement. Pursuant to CIP 010-2 section (1.3), any changes deviating from the baseline configuration must be tested and verified. In this case, because "SecureController" is custom code, it should

have been tested properly and the security vulnerabilities discovered. It should not have made it into the production environment.

**Recommendations**

User Account Control and Internet Explorer Enhanced Security Configuration should remain enabled. Explicit permission should be given before installation of new software.

## Redis Server Accessible from Corporate Network

| Finding ID | Severity | Affected Hosts | NERC/CIP Regulation | CVE |
|---|---|---|---|---|
| H-02 | 7.1 (High) | 10.0.10.31 | CIP 005-5<br>CIP 007-6 | N/A |

### Description

Team [redacted] discovered that a Redis server, very likely used to store data related to programmable logic controllers, was accessible from the corporate network. Although the server is password protected, it has minimal protection against brute force attacks. With access to Redis, it's likely that an attacker could gain remote code execution on the machine, and have subsequent access to read and write to programmable logic controllers.

### Impact

Brute force attacks on redis across a corporate intranet allow for many thousands of attempts per minute, and with additional time team [redacted] may have been able to crack the password. Once a threat actor has gained access to redis, there are various ways to gain remote code execution. With remote code execution, the programmable logic controllers on the same subnet would be able to be written to and read from, representing a severe threat of service disruption and loss of human life. Even without remote code execution, additional service interruption may be possible; although Team [redacted] did not have the access to verify it, it's likely the values on this server are a temporary storage for values read from the PLCs. Modifying these could introduce false values and induce an administrator into making decisions on false data.

### Steps to Reproduce

An nmap scan from a machine inside the corporate network reveals the existence of the machine and open port:

```
$ nmap 10.0.10.0/24
...
Nmap scan report for ip-10.0.10.31.internal (10.0.10.31)
Host is up (0.00071s latency)
Not Shown: 65534 filtered ports
PORT     STATE SERVICE
6379/tcp open  redis
```

The team then used Hydra:

```
$ $ hydra -P
/usr/share/SecLists/Passwords/xato-net-10-million-passwords-1000000.txt
10.0.10.31 redis
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is
non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-01-10
04:03:47
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1000000 login tries
(l:1/p:1000000), ~62500 tries per task
[DATA] attacking redis://10.0.10.31:6379/
...
```

The attempt to brute-force the password was ultimately unsuccessful.

### Finding Comments

A warning from an example redis configuration from https://download.redis.io/redis-stable/redis.conf

```
# Warning: since Redis is pretty fast, an outside user can try up to
```

```
# 1 million passwords per second against a modern box. This means that you
# should use very strong passwords, otherwise they will be very easy to break.
# Note that because the password is really a shared secret between the client
# and the server, and should not be memorized by any human, the password
# can be easily a long string from /dev/urandom or whatever, so by using a
# long and unguessable password no brute force attack will be possible.
```

### Recommendations

The developers of redis recommend that "Access to the Redis port should be denied to everybody but trusted clients in the network, so the servers running Redis should be directly accessible only by the computers implementing the application using Redis"(https://redis.io/topics/security). The redis server should only be accessible by the HMI backend web application (`10.0.10.15`). This could be accomplished with a firewall on the redis server machine. A strong password and username should be used. The link above provides additional recommendations.

Alternatively, the redis server could be taken off the network entirely. The resource utilization of the server is likely quite low given the team's knowledge of the application, and thus could probably be moved to the same machine running the web application that accesses it on 10.0.10.15. The server should then communicate with redis via a unix domain socket.

# Medium Severity Findings

## Insufficient Password Policy

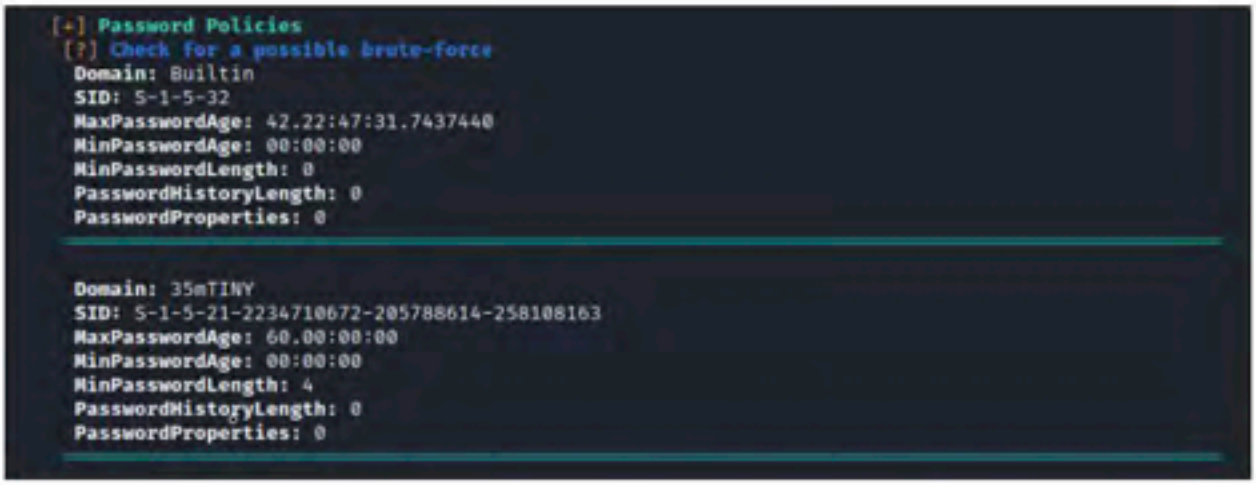
| Finding ID | Severity | Affected Hosts | NERC/CIP Regulation | CVE |
|---|---|---|---|---|
| M-01 | 5.9 (Medium) | 10.0.1.10-13, 10.0.5.50 | NERC/CIP 007-6 | N/A |

### Description

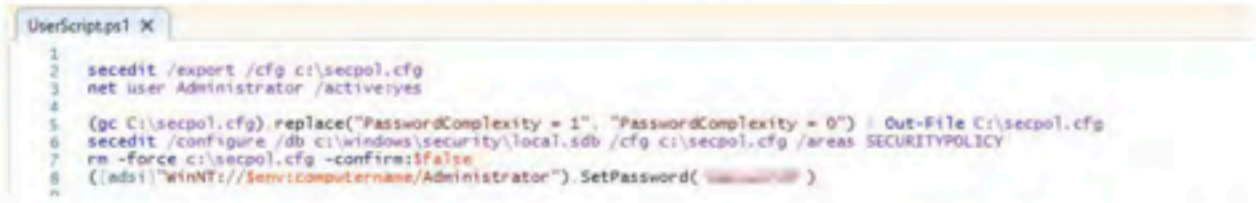
Weak password policies were identified on NGPEW workstations creating insufficient account lockout time periods and instances of poor password complexity throughout the environment.

### Impact

All NGPEW corporate workstations (`10.0.1.10-13`) are subject to weak password policies. These policies significantly reduce the baseline security level of the machines.




The existing policies do not adhere with NERC/CIP standards and allow users to set passwords as short as 4 characters long. Additionally, password complexity is not enforced leading to the use of extremely simple passwords.




Team [redacted] took advantage of this configuration to bruteforce administrator credentials on the corporate workstations as seen in Findings C-03 and C-03a.

### Steps to Reproduce

Password policy information was pulled through the use of winPEAS (Windows Privilege Escalation Awesome Scripts by carlospolop, available on GitHub). The command, `net accounts`, can also be used to pull the password policy on the machine.

### Finding Comments

A weak password policy significantly increases the likelihood of a successful brute-force attack. The lack of password complexity allowed Team [redacted] to access NGPEW workstations by simply guessing the administrator password.

### Recommendations

High password complexity should be enforced as part of security enforcement throughout the network.

NERC/CIP 007-6 (Sections 5.5, 5.6, 5.7) requires the following password complexity:

**Section 5.5**: at least 8 characters (or maximum supported by asset), character complexity (at least 3 of upper/lowercase, numeric, non-alphanumeric).
**Section 5.6**: password rotation (`MinPasswordAge`) enforced at least once every 15 months.
**Section 5.7**: limit to or alerting from unsuccessful logins (expect to report on systems that don't enforce limited logon attempts).

## Password in Cleartext Communication and Storage

| Finding ID | Severity | Affected Hosts | NERC/CIP Regulation | CVE |
|---|---|---|---|---|
| M-01a | 5 (Medium) | 10.0.1.12 | CIP-004-6 | N/A |

### Description

Team[redacted] while having administrative access to the host 10.0.1.12, was able to access email application storage files. These files contained copies of inbox and sent email messages. In one of the exchanges a password to a VNC server was sent in clear text.

### Impact

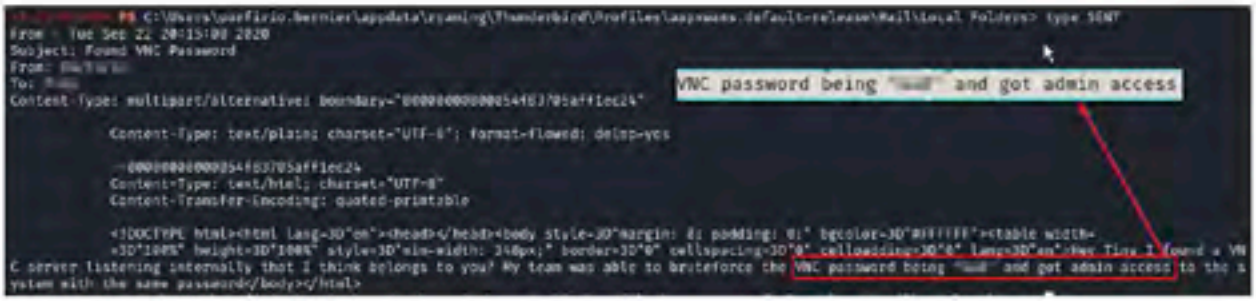
Team[redacted] was not able to utilize the acquired password to compromise any known service on the network, so the impact in this specific case was low. In general, cleartext passwords can result in the compromise of sensitive data, and access, and has the potential to result in significant financial loss and real world damage.

### Steps to Reproduce

Log in as administrator on one of the workstation hosts and access the INBOX and SENT files in the following folder:

```
C:\Users\[user]\appdata\roaming\Thunderbird\Profiles\aapxwams.default-release\Mail\Local
```

On Porfirio's workstation the following was found:




### Recommendations

Sharing passwords over email is a common practice; however several security measures need to be implemented in order to communicate securely over the network. Email storage is usually not encrypted. If there is a need to share a password through email or other cleartext avenues, there are a few ways to do it. Installing a password manager, such as LastPass or 1Password, or The first is preferable because it deals immediately with two issues - secure communication and password management.

Using a password manager will generate a complex and secure password every time a user logs in and saves it in encrypted form and is accessible across multiple devices. It also has a function of secure password share across insecure networks, such as the Internet. However, it has a downside - an agent has to be installed on both sending and receiving devices. Another way is to encrypt email with PGP. The most available is to use OpenPGP. Employees should also be educated not to share cleartext passwords.

## Windows Defender Real-Time Protection Disabled

| Finding ID | Severity | Affected Hosts | NERC/CIP Regulation | CVE |
|---|---|---|---|---|
| M-02 | 5.5 (Medium) | 10.0.1.10-13 | CIP 007-6 | N/A |

### Description

Upon accessing corporate (`corp.millenialpower.us`) workstations (`10.0.1.10-13.corp.millenialpower.us`) via Remote Desktop, it was identified that Windows Defender Real-Time Protection was disabled.

### Impact

All identified corporate machines had Windows Virus & Threat protection and Windows Defender Real-Time Protection disabled.

These machines include `10.0.1.10` used by Grace Grantham, `10.0.1.11` (Gaylord Schaefer), `10.0.1.12` (Tiny Glover), and `10.0.1.13` (Porfirio Bernier).

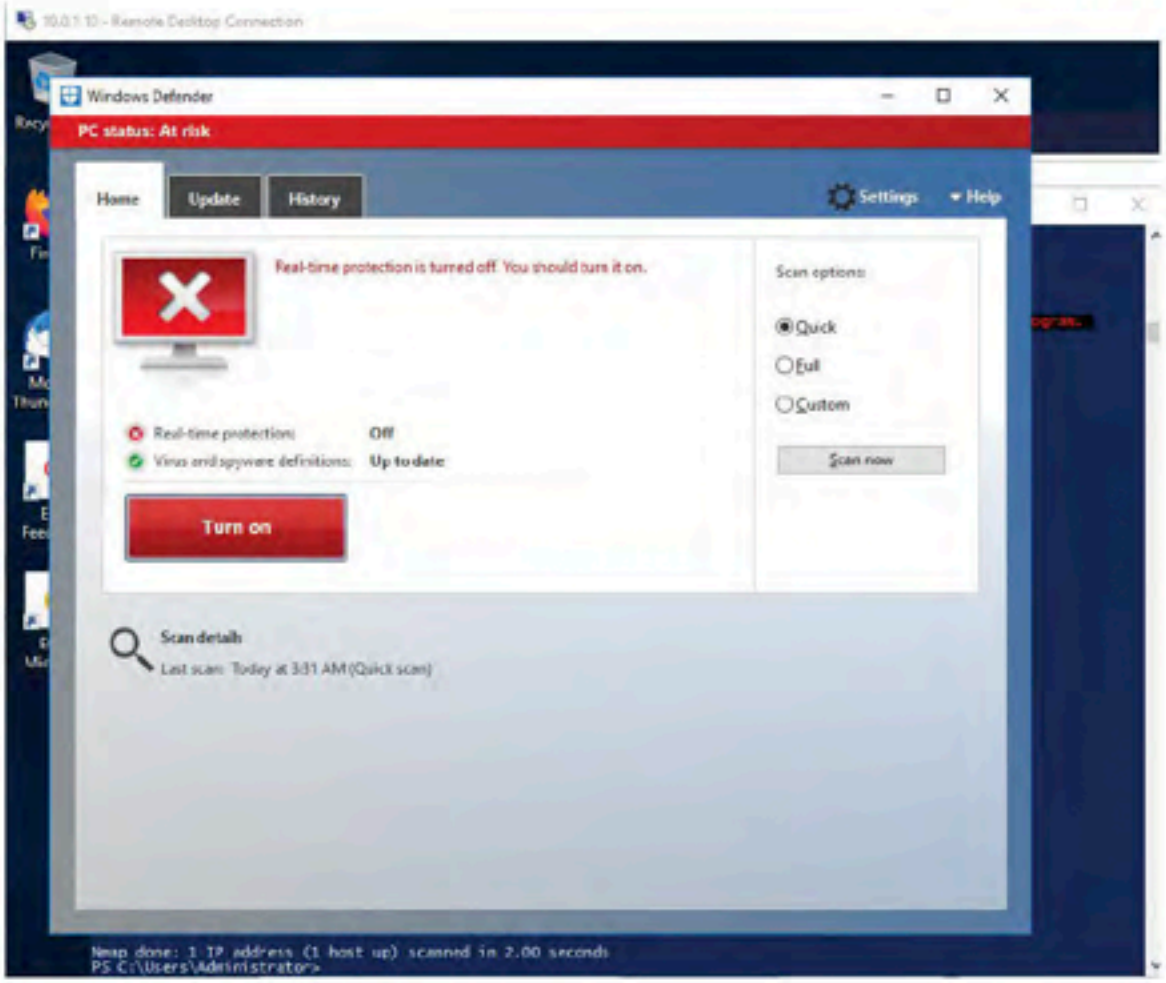



*Fig.1: Real-Time Protection disabled on `10.0.1.10` (grace). Device at risk.*

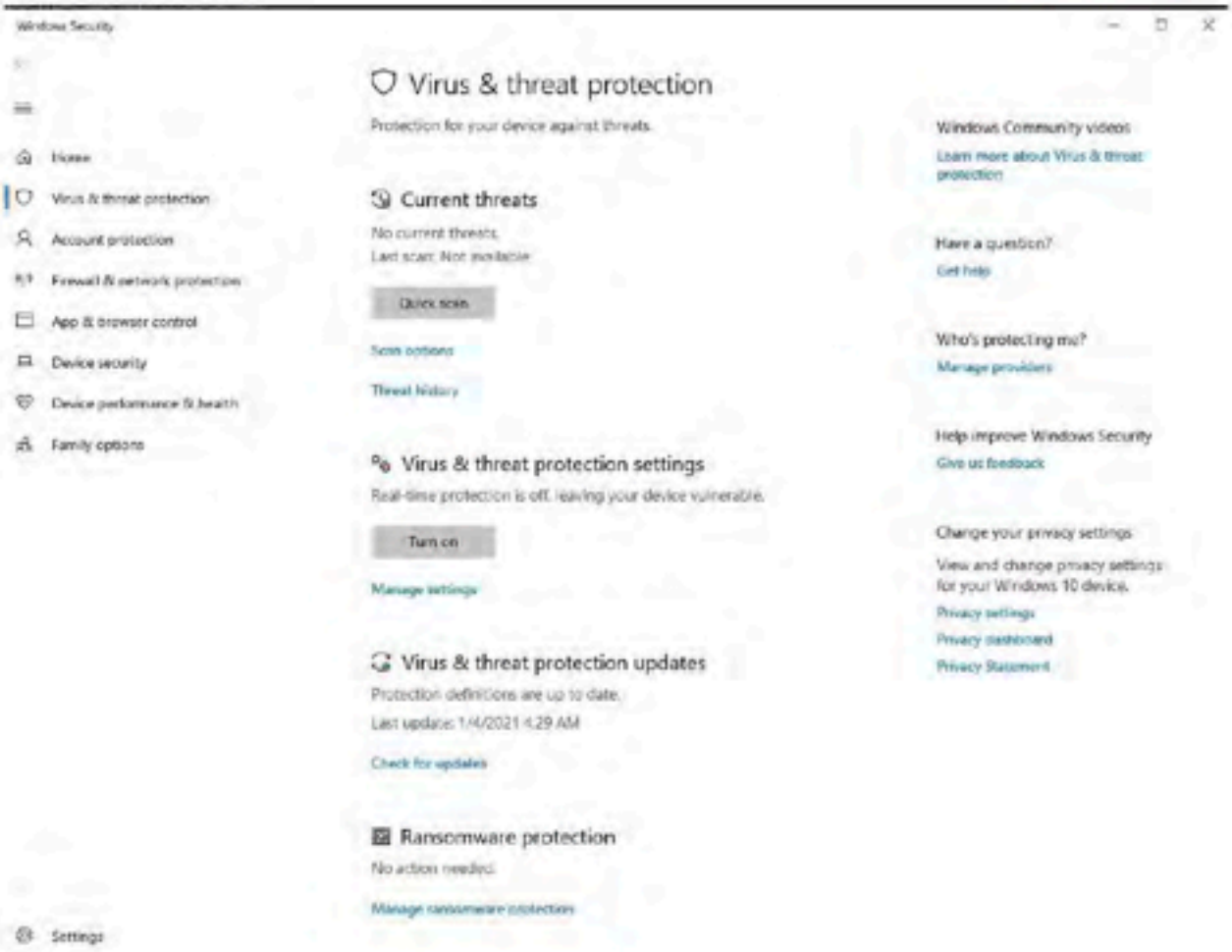



*Fig. 2: Virus & Threat protection turned off on `10.0.1.10` (grace)*

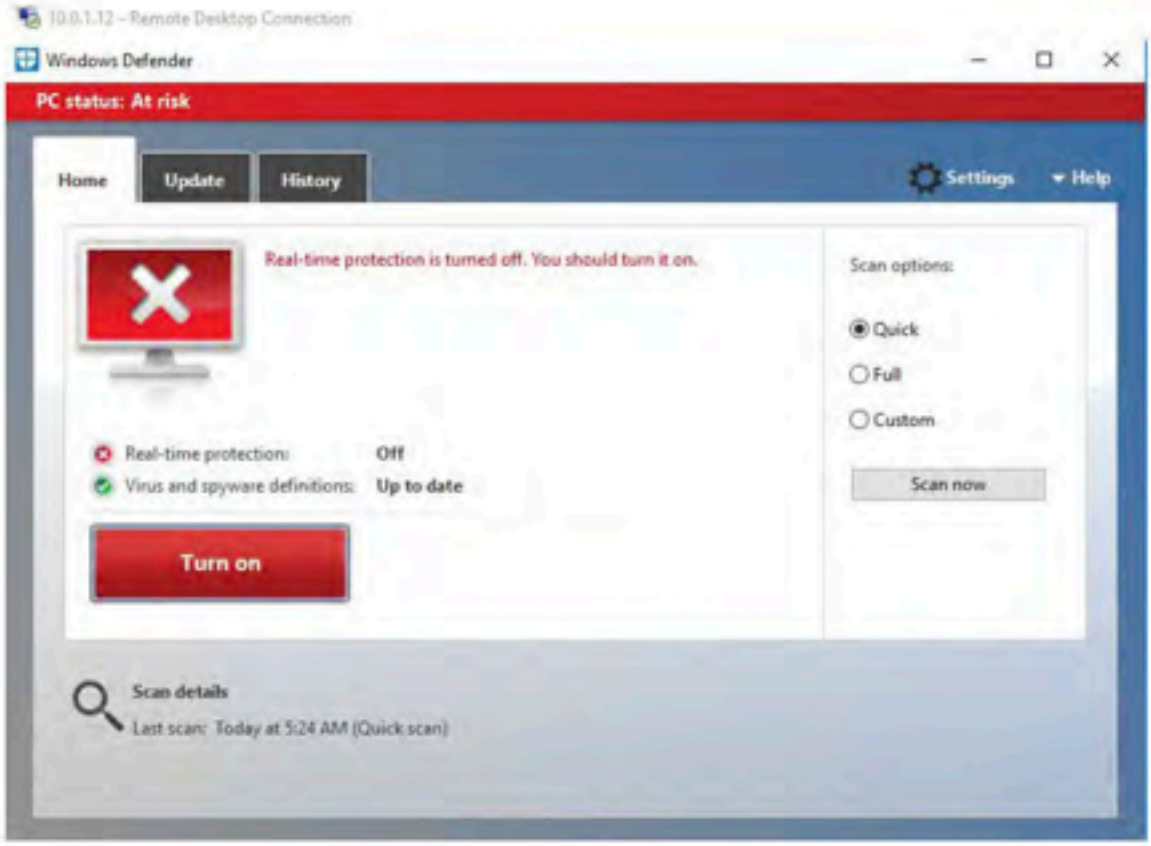



*Fig. 3: Real-Time Protection disabled on `10.0.1.12 (tiny)`. Device at risk.*

The lack of real-time protection on the machines significantly reduces the complexity required for potential attacks and reduces the visibility of malicious activity on the machines.

### Steps to Reproduce

Windows Security settings can be viewed by clicking the shield icon in the task bar or searching the start menu for Defender. Click the Virus & threat protection tile (or the shield icon on the left menu bar) to view configuration details.

### Finding Comments

Built-in security protections should not be disabled if they don't have to be. This misconfiguration allowed for the unrestricted use of enumeration and exploitation tools on the affected machines including `WinPEAS.exe` (Windows Privilege Escalation Awesome Scripts).

### Recommendations

Windows Defender provides a baseline level of defense on Windows machines and should remain up-to-date and enabled unless compatibility issues occur with alternative, corporate antivirus solutions installed on the machine. As described by Microsoft, "Windows Security continually scans for malware (malicious software), viruses, and security threats. In addition to this real-time protection, updates are downloaded automatically to help keep your device safe and protect it from threats." The effective use of antivirus software is required by CIP 007-6, Section (3.1).

## Public Company Hierarchy visible through GitHub Repository History

| Finding ID | Severity | Affected Hosts | NERC/CIP Regulation | CVE |
|---|---|---|---|---|
| M-03 | 5.2 (Medium) | N/A | CIP 004-6 | N/A |

### Description

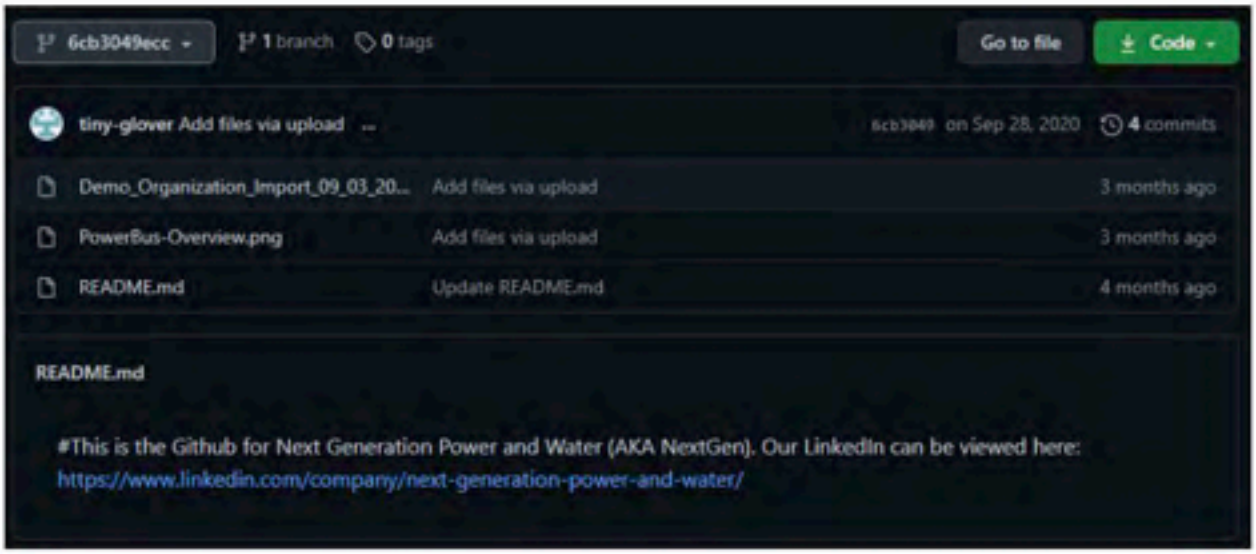
During the engagement, Team [redacted] discovered that attackers can gain access to files on the NGPEW github repos that were previously "deleted." Although the organizational hierarchy and the PowerBus overview were deleted in a commit in the GitHub repository, they are still visible via the repository history. These documents contain sensitive information that should not be shared publicly.

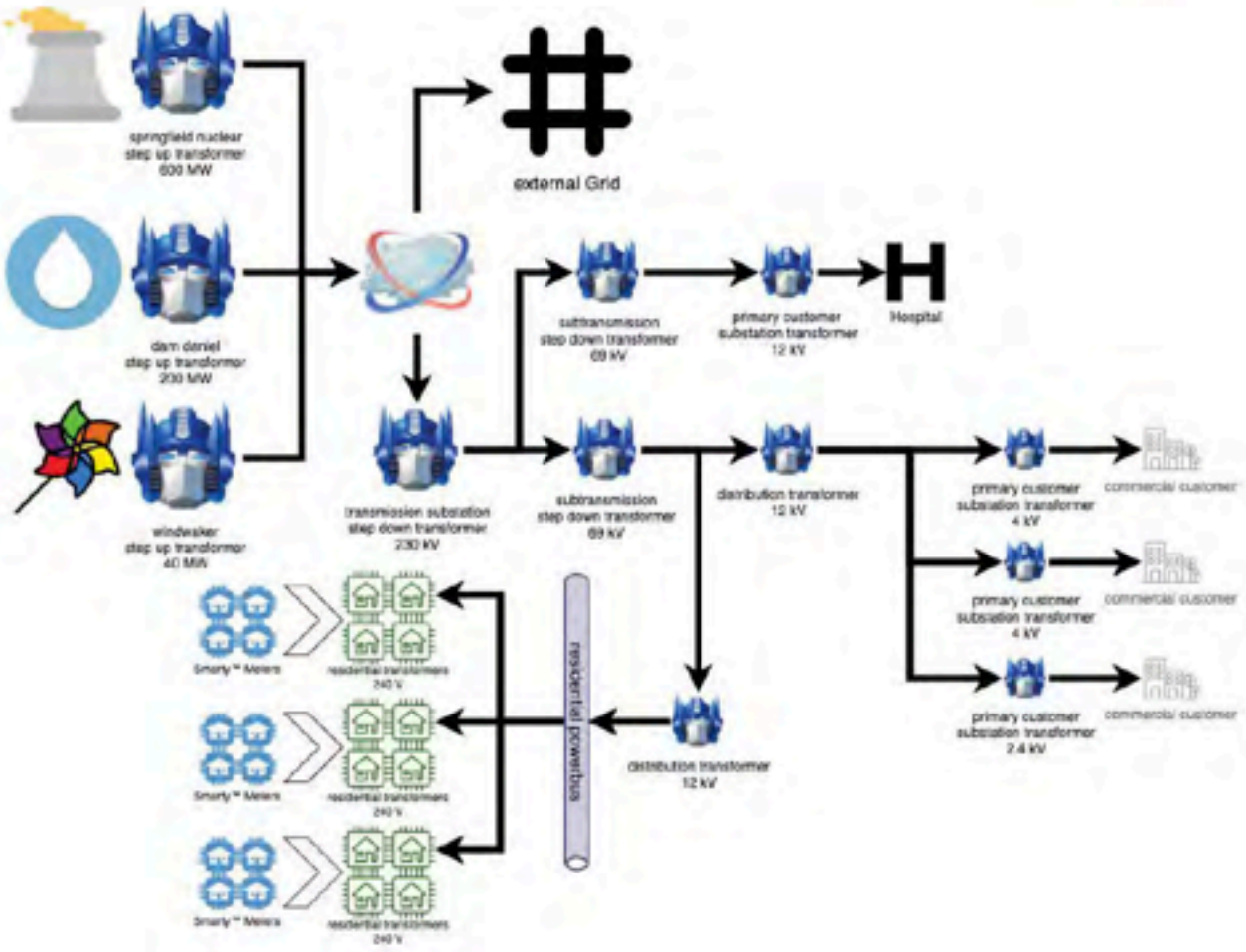
### Impact

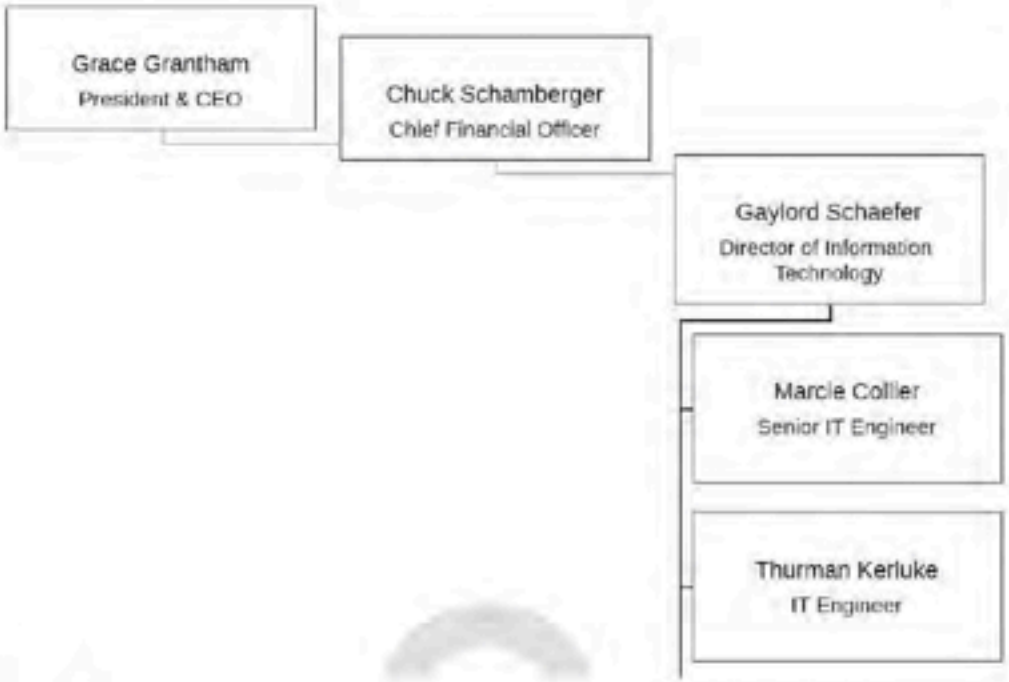
Due to the fact that this GitHub repository is public, anyone could have access to potentially harmful information. This could lead to more sophisticated social engineering attacks and subsequent compromise of sensitive devices and information.

### Evidence and Steps to Reproduce

By navigating to the public NGPEW github, https://github.com/Next-Generation-Power-and-Water, and clicking "Docs", "commits", September 28th "Add files via upload" by tiny-glover, then "Browse files", an attacker can still gain access to these deleted documents.


6cb3049ecc
1 branch
0 tags
Go to file
Code
tiny-glover Add files via upload ...
6cb3049 on Sep 28, 2020
4 commits
Demo_Organization_Import_09_03_20...
Add files via upload
3 months ago
PowerBus-Overview.png
Add files via upload
3 months ago
README.md
Update README.md
4 months ago
README.md
#This is the Github for Next Generation Power and Water (AKA NextGen). Our LinkedIn can be viewed here:
https://www.linkedin.com/company/next-generation-power-and-water/


springfield nuclear
step up transformer
600 MW
external Grid
dam daniel
step up transformer
200 MW
windwaker
step up transformer
40 MW
transmission substation
step down transformer
230 kV
subtransmission
step down transformer
69 kV
primary customer
substation transformer
12 kV
Hospital
subtransmission
step down transformer
69 kV
distribution transformer
12 kV
primary customer
substation transformer
4 kV
commercial customer
primary customer
substation transformer
4 kV
commercial customer
primary customer
substation transformer
2.4 kV
commercial customer
distribution transformer
12 kV
residential powerbus
Smarty™ Meters
residential transformers
240 V
Smarty™ Meters
residential transformers
240 V
Smarty™ Meters
residential transformers
240 V




**Recommendations**

CIP 004-6 maintains five main requirements for personnel, one of which is a Security Awareness Program. To fulfill this requirement, Team [redacted] recommends expanding the current NGPEW Security Awareness Program to include employee training to refrain from disclosing potentially sensitive information on outside code repositories such as GitHub.

Additionally, Team [redacted] recommends either an immediate deletion of the entire repository, or the conversion of the repository to private. Team [redacted] also recommends a presentation on the importance of good operational security in the workplace.

## Non-Domain-Joined Workstations

| Finding ID | Severity | Affected Hosts | NERC/CIP Regulation | CVE |
|---|---|---|---|---|
| M-04 | 4.2 (Medium) | 10.0.1.10-13 | CIP 010-2 | N/A |

### Description

Corporate workstations are not joined to the `corp.millenialpower.us` domain. A Domain Controller at `10.0.1.100` was discovered and is active.

### Impact

The lack of centralized configuration via a Domain Controller led to inconsistent configurations of user workstations throughout the environment as seen in finding H-01 and C-03.

The presence of non-domain-joined machines throughout the network reduces visibility of active machines and increases the effort required to properly maintain consistent device configurations.

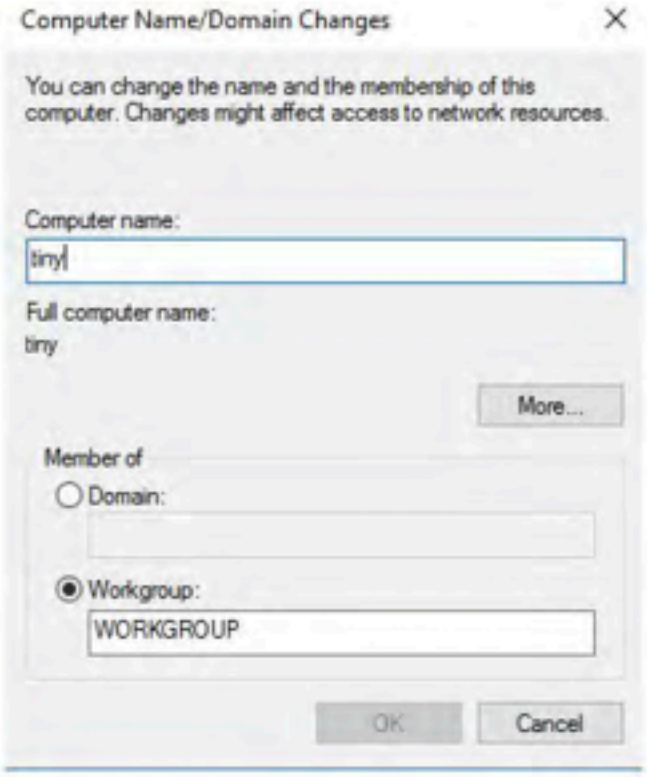



*Fig. 1: `10.0.1.12` (`tiny`) not joined to the domain.*

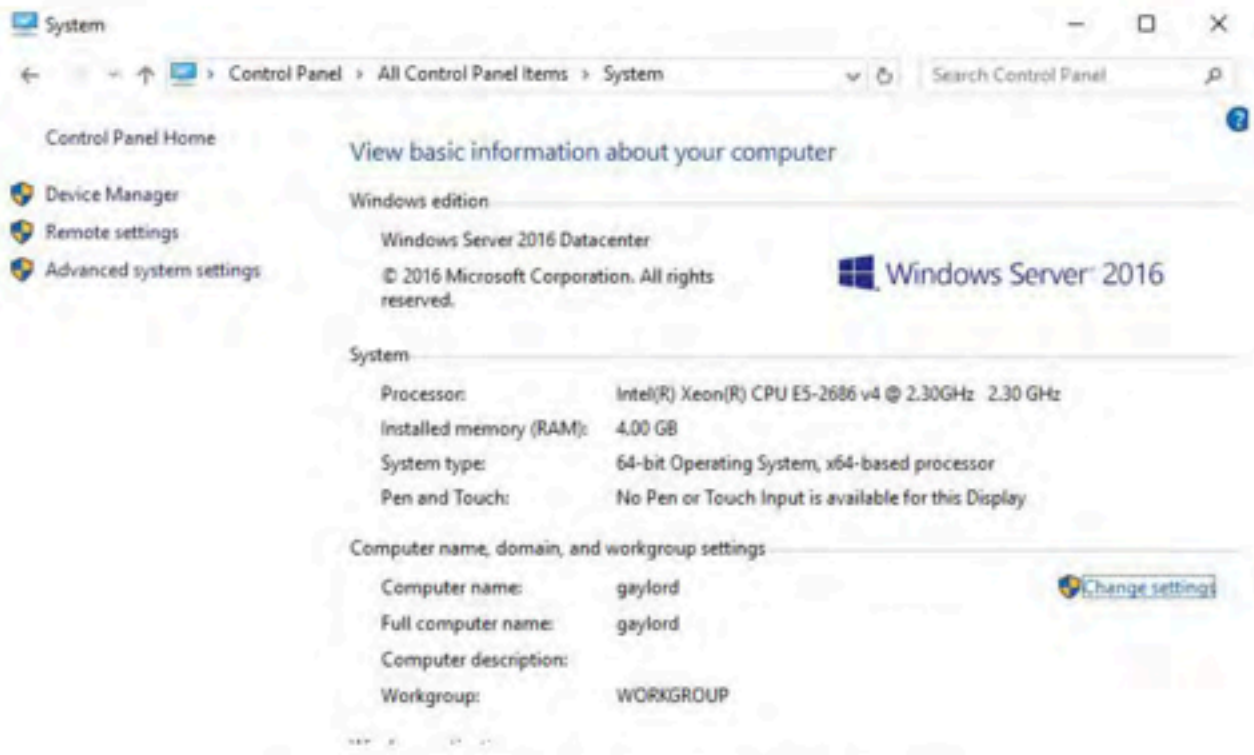



*Fig. 2: `10.0.1.11` (`gaylord`) not joined to the domain.*

### Steps to Reproduce

Team [redacted] queried domain information once connected with the identified local administrator. The domain of each machine can be identified by `sysdm.cpl` or by running `wmic computersystem get domain`. Additionally, domain joined machines will be visible from the Domain Controller within Active Directory.

### Finding Comments

Since the workstations were not joined to the domain, we were unable to utilize compromised workstations to pivot to the domain controller as anticipated. Domain Administrator accounts were not discovered and domain enumeration via BloodHound proved to be ineffective.

**Recommendations**

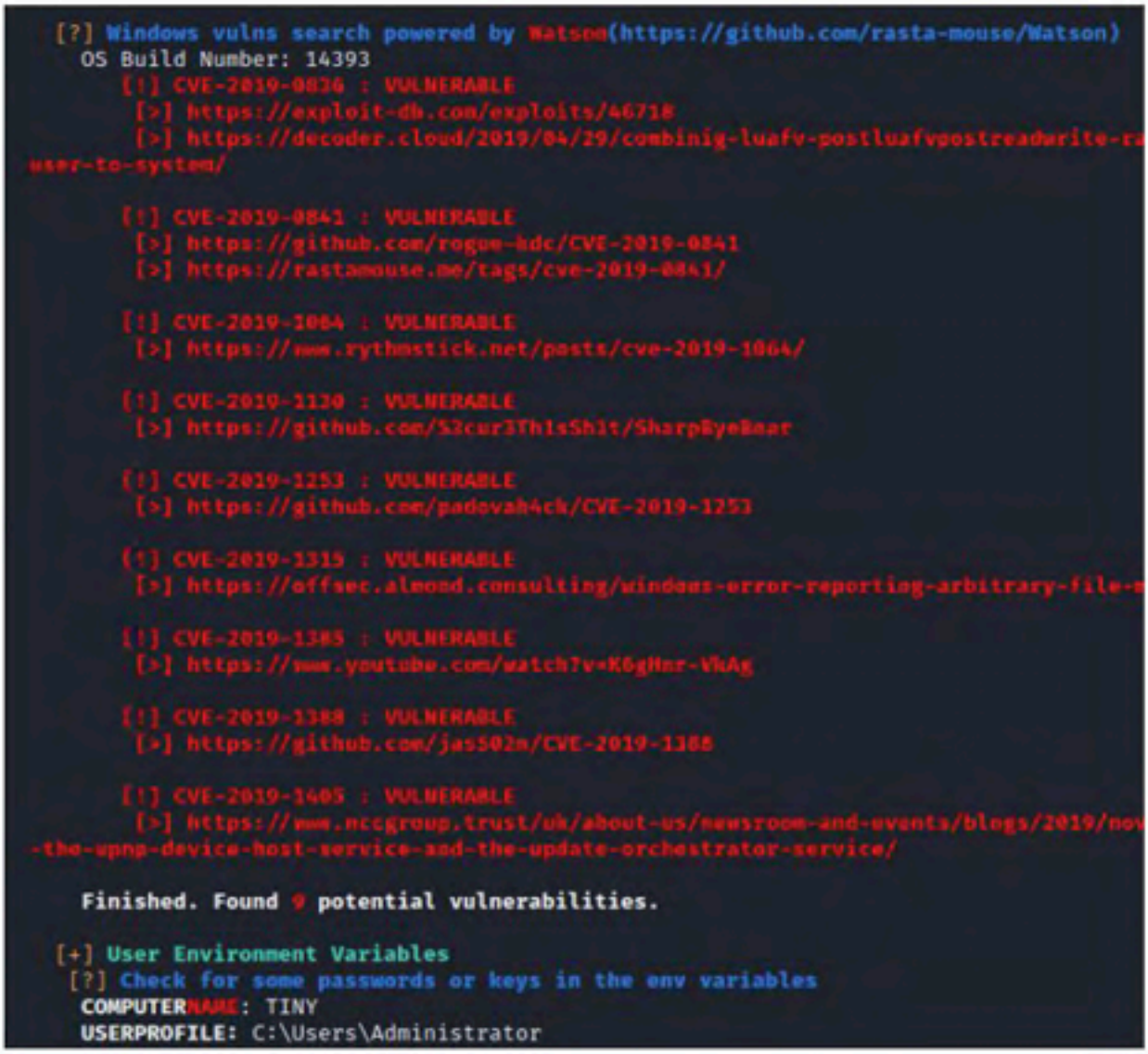
All user workstations should be connected to the corporate domain to allow standardized device administration via the Domain Controller. The use of scripts to administer device policy and settings can be mitigated by applying Group Policy across the domain. CIP 010-2 recommends to "develop a baseline configuration, individually or by group, which shall include Operating systems … or firmware where no independent operating system exists."

## Workstation Patch Status

| Finding ID | Severity | Affected Hosts | NERC/CIP Regulation | CVE |
|---|---|---|---|---|
| M-05 | 4.2 (Medium) | 10.0.1.10 - 10.0.1.13 | CIP 010-2<br>CIP 007-6 | Various |

### Description

[redacted] discovered that the four workstations on `10.0.1.10 - 10.0.1.13` network were running Windows Server 2016 build 14393. Although this build is still in mainstream support, its age has allowed for many vulnerabilities to be discovered, as evidenced by a WinPEAS scan.




### Finding Comments

Team [redacted] was not able to determine the exact Windows version with nmap before gaining administrator access to the host (finding C-03).

```
Nmap scan report for ip-10-0-1-11.ec2.internal (10.0.1.11)
Host is up, received echo-reply ttl 128 (0.0014s latency).
Scanned at 2021-01-08 14:47:41 UTC for 170s
Not shown: 996 closed ports
Reason: 996 resets
PORT     STATE SERVICE       REASON          VERSION
135/tcp  open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
139/tcp  open  netbios-ssn   syn-ack ttl 128 Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  syn-ack ttl 128 Microsoft Windows Server 2008 R2 - 2012
microsoft-ds
3389/tcp open  ms-wbt-server syn-ack ttl 128 Microsoft Terminal Services
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE:
cpe:/o:microsoft:window
```

### Recommendations

Pursuant to CIP 010-2 a baseline, standardized configuration needs to be developed pertaining to OS version. When new updates, versions, or software is released, there should be a documented process in which the change can be authorized, tested, and approved for deployment into the production environment.

Pursuant to CIP 007-6 Section (2.2), security patches should be evaluated every 35 days. These workstations should be evaluated and upgraded according to the System Security Management documentation.
Upgrade to the latest Microsoft Windows Server NT 10.0, build 19041.

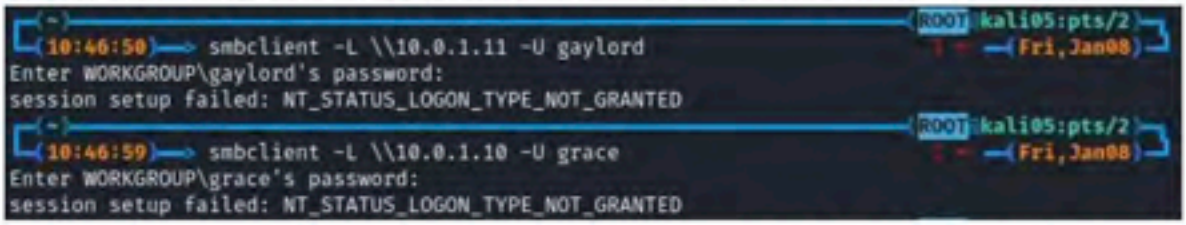
# Appendix A - Hosts and Open Ports

| [redacted] | [redacted] |
|---|---|
| 10.0.1.0/24 | |
| 10.0.1.1 | |
| 10.0.1.10 | 135, 139, 445, 3389, 5985, 9971, 47001, 49664, 49665, 49666, 49668, 49669, 49675, 49678 |
| 10.0.1.11 | 135, 139, 445, 3389, 5985, 9971, 47001, 49664, 49665, 49666, 49668, 49669, 49675, 49678 |
| 10.0.1.12 | 135, 139, 445, 3389, 5985, 9971, 47001, 49664, 49665, 49666, 49668, 49669, 49675, 49678 |
| 10.0.1.13 | 135, 139, 445, 3389, 5985, 9971, 47001, 49664, 49665, 49666, 49668, 49669, 49675, 49678 |
| 10.0.1.60 | 22 (Closed: 80, 443) |
| 10.0.1.100 | 53, 88, 135, 389, 445, 464, 636, 3268, 3269, 3389, 49152 (Closed: 123), UDP: 53, 123, 389 |
| 10.0.1.154 | 22, 3000 (Closed: 80, 443) |
| 10.0.1.198 | |
| 10.0.2.199 | |
| 10.0.2.200 | |
| 10.0.2.201 | |
| 10.0.2.202 | |
| 10.0.1.203 | |
| 10.0.5.0/24 | |
| 10.0.5.50 | 135, 139, 445, 3389, 5900 |

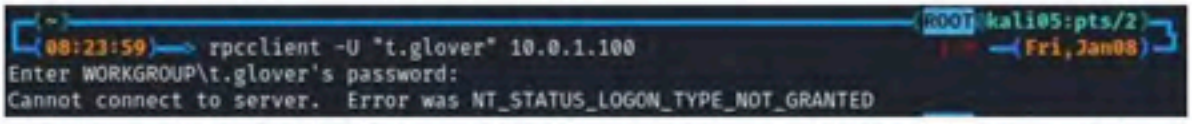
| | |
|---|---|
| 10.0.5.75 | 80, 3306, 8000, 8080, 12345 (Closed: 443, 9090) |
| 10.0.5.151 | 22, 3306 (Closed: 80, 443, 5432, 27017, 27018, 27019) |
| 10.0.5.152 | 80, 135, 443, 5900 (Closed: 22, 123, 389, 445, 464, 3389, 5800) |
| 10.0.5.153 | 22, 80 (Closed: 443) |
| 10.0.10.0/24 | |
| 10.0.10.15 | 80 |
| 10.0.10.30 | 3040 |
| 10.0.10.31 | 6379 |
| 10.0.10.50 | 502 |
| 10.0.10.51 | 502 |
| 10.0.10.52 | 502 |
| 10.0.10.53 | 502 |
| 10.0.10.55 | 502 |
| 10.0.10.56 | 502 |
| 10.0.10.57 | 502 |
| 10.0.10.59 | 502 |
| 10.0.10.60 | 502 |
| 10.0.10.61 | 502 |
| 10.0.10.62 | 502 |
| 10.0.10.63 | 502 |
| 10.0.10.64 | 502 |
| 10.0.10.65 | 502 |

# Appendix B - Infrastructure Strengths

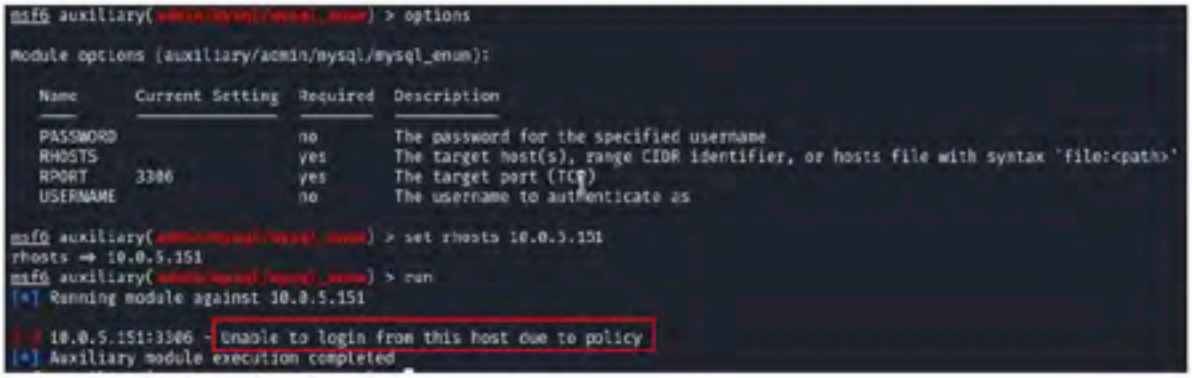
1. SMB shares on the host computers were not accessible to anyone not on the subnet and the remote logon type with smbclient was not allowed.



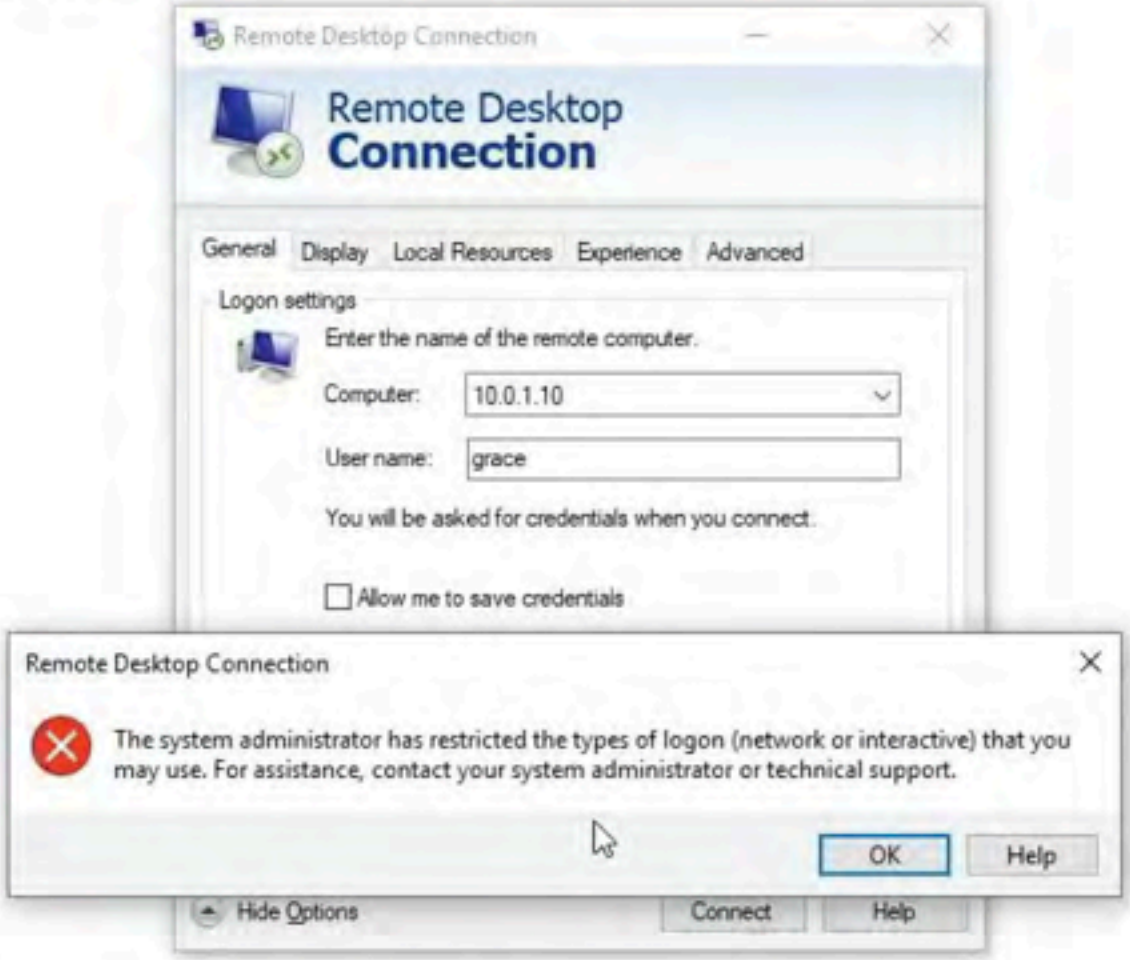

2. RPC hosts were not accessible to anyone not on the subnet and the remote logon type with rpcclient was not allowed.




3. Mysql server on 10.0.5.151 on port 3306 was not accessible to anyone except for a specific service.



4. Remote desktop protocol was disabled for all users except the Administrator on the hosts.




5. Security box 10.0.1.60 had an up-to-date version of Linux Ubuntu 20.04.1

6. NGPEW primarily uses updated versions Windows Server 2016 and does not utilize more vulnerable versions such as Windows 2012 R2 or Windows 2008.


7. The team also discovered that EternalBlue and BlueKeep scans do not detect any servers vulnerable to the exploits.

# Appendix C - Severity and Risk Calculation

Severity and Risk calculations are numerical scores based on quantitative methods. We used the NIST CVSS standard to evaluate and organize the findings in our report. Findings are ranked on a score from 0 to 10, from lowest to highest levels of severity. Contributing factors to base level severity include attack vector, attack complexity, privileges and user interaction required, as well as impacts to confidentiality, integrity, and availability. CVSS ratings are also evaluated based on environmental risk factors, which add a considerable amount of severity in an environment consisting of Distributed Control Systems.

**Severity = Average (Impact Score + Vulnerability Level)**

- Critical (8.0 - 10.0)
- High (6 - 7.9)
- Medium (4.0 - 5.9)
- Low (0 - 3.9)

*Example:* (7.5+6.5)/2 = 7, Severity: High Risk

Component Definitions

Impact Score - Scored according to loss of Confidentiality, Integrity, Availability, and Accountability in regards to data pertaining to NGPEW. Include Financial, Reputational, Non-Compliance, and Privacy impact.

Vulnerability Level - Scored according to likelihood of exploitation and the following impact to the affected device. Factors include ease of discovery, exploit sophistication, available public disclosures, system impact, associated devices, and IDS evasion.

# Last Page