NEXT GEN

Next-Generation Power, Electric & Water Penetration Report

January 2021

Finals [redacted]

Table of Contents

Executive Overview

This penetration test was conducted on *January 7-9*, 2021 on behalf of Next-Generation Power, Electric & Water (NGPEW).

Goals

1. Assess the security posture of NGPEW's internal network from a provided set of assets
2. Verify the remediation of findings from the previous October assessment
3. Assess findings in relation to compliance with CIP standards

Finding Severity

Critical	1
High	6
Medium	5
Low	2
Informational	3

Timeline

Network Assessment
January 7-9

Presentation and Delivery of Assessment Findings
January 10

Core Observations

Throughout the engagement, it was evident that NGPEW values improving their operational security. The presence of intrusion detection and prevention system tools such as Splunk and Suricata are examples of such. The company choosing to allocate a portion of the monetary donation received from LexCorp to hire consulting services illustrates that security is a priority.

Some of the fundamental lapses in security that threaten NGPEW's security posture include misconfigurations of existing intrusion detection and prevention software, vulnerable password policies, incorrect storage of sensitive data, and a lack of network segmentation. The risks associated with these types of vulnerabilities could damage NGPEW's reputation as a regional supplier of water and electricity and also carry financial consequences in a worst case scenario. As such, NGPEW can increase their security posture even further by resolving the technical findings as disclosed in this vulnerability assessment.

Since our first engagement, NGPEW has increased their security posture by remediating several significant vulnerabilities as described in our previous assessment. During this engagement, it was observed that the Operational Technology network was now segmented from the Corporate network as

recommended by the testing team. The anti-malware and antivirus program, Windows Defender was present on the hosts running Windows operating system, which is a notable security measure enhancement as previously any such software was not encountered on any available assets. Sensitive information such as user credentials and system logs were no longer available through the reproduction steps as previously reported. These are just some of the examples of the changes that greatly benefited NGPEW's operational security that demonstrate the companies' dedication to providing persistent services.

Compliance

Given NGPEW's status as a power provider in North America, NGPEW must be compliant with North American Electric Reliability Corporation (NERC)'s standards for Critical Infrastructure Protection (CIP). These standards were assessed in conjunction with this assessment and details are included with relevant findings. Relevant documentation as referenced throughout this document can be found on NERC's public website[1]. The two documents most thoroughly referenced in this assessment are CIP-005-6[2] and CIP-007-6[3].

Scope

The scope of this penetration test given by Next-Generation Power and Water were the `10.0.1.0/24` `10.0.5.0/24` and `10.0.10.0/24` IP ranges. Any assets not in this range were not audited and this document should not be used to speak for their security. In addition, the `10.0.254.0/24` IP range was specifically excluded per the contractual agreement. The consulting team's initial access was from the `10.0.254.0/24` subnet which only had access to the `10.0.1.0/24` network, as such we recommend similar engagements where the consultants were given access to different networks initially to fully evaluate the other networks and emulate different attack situations. During the assessment, additional access to a scanning host at `10.0.1.60` with user `pentest` was provided at 1:07PM EST on January 9th for use in the engagement.

Due to the sensitive nature of the critical systems within the network, a cautious approach was taken to ensure the penetration test stayed within the agreed scope. Being an energy-sector company, the team remained cognizant to not disrupt or modify any services as it could result in disruption to NGPEW's customers. In addition, any personally identifiable information (PII) that relates to the company's

[1] https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
[2] https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-005-6.pdf
[3] https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-007-6.pdf

customers or employees were handled with caution - it was ensured that data was not exfiltrated out of the Next Generation Power and Water internal network and/or provided assets.

Executive Recommendations

Below, three core recommendations are listed from this assessment. These do not replace the remediation recommendations listed per each finding but supplement them.

Implement Strong Authentication Systems

As per CIP-005-6 part 2.3, NGPEW should "require multi-factor authentication for all interactive remote access sessions" to High impact Bulk Electric System (BES) Cyber Systems, Medium Impact BES Cyber Systems with External Routable Connectivity, and all associated Protected Cyber Assets. During the assessment, no evidence of any multi-factor authentication systems was found, even when interacting directly with BES systems. In addition, multiple credentials found throughout the assessment were of a low quality and did not match industry standards for password complexity.

Improve Network Segmentation

Network Segmentation between corporate assets and BES assets in the assessed network was completed using AWS's Security Groups. These were configured initially to restrict access from VDI systems to only the corporate network. When provided with the scanning host `10.0.1.60`, we determined that 10.0.1.60 could communicate with all three networks (`10.0.1.0/24`, `10.0.5.0/24`, and `10.0.10.0/24`) with only a single IP address on the corporate network (`10.0.1.0/24`). As such, a machine on the corporate network is able to communicate with critical BES assets given proper configuration. In order to protect NGPEW's critical BES systems, we recommend stronger segmentation of corporate and BES networks through either the use of a secure jump host requiring multi-factor authentication or air gapping the BES networks.

Improve Network Visibility and Firewalls

During the assessment, the team discovered that external domains were accessible from the internal network. One such domain was the code repository Github. Monitoring and filtering egress traffic allows for careful inspection and monitoring of any and all traffic, intellectual property, and possible threats leaving the NGPEW network. By restricting, inspecting, and managing network access via packet filtering, NGPEW can increase its corporate security posture. This will also allow for greater ease of access to historical threat context and intelligence. According to Requirement 1 of CIP-005-6, "The [Electronic

Access Point] should control both inbound and outbound traffic.[4] Enabling egress traffic filtering and monitoring would further NGPEW's compliance with CIP standards.

[4] Page 18: CIP-005-6

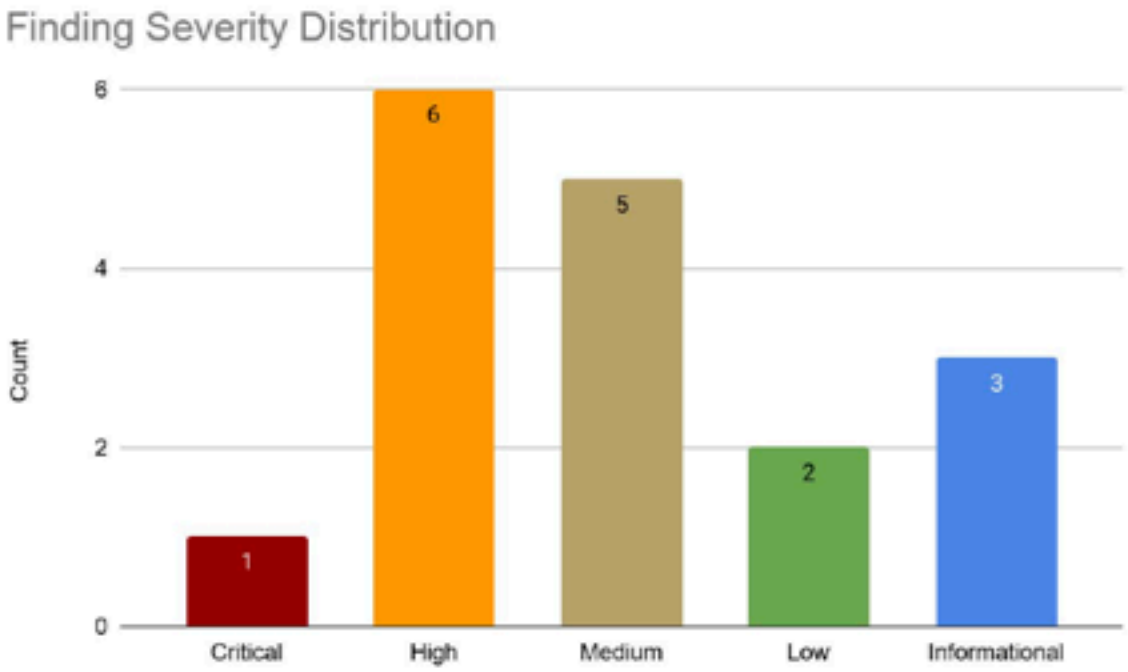
Technical Briefing

Technical Summary

The risk assessment of the technical findings in the subsequent sections is evaluated in accordance with the definitions as supplied by the Common Vulnerability Scoring System (CVSS). The CVSS provides a numerical score ranking severity by three different metrics. The CVSSv3 evaluation metrics apply to a vulnerability's constant intrinsic qualities, chronological characteristics, and uniqueness to the user environment respectively. The resulting calculation is a value between 0 and 10, ranking the given vulnerability from a low criticality to the highest severity. Per each finding, a footnote is provided with the full CVSS v3 score for the finding. A detailed table of the CVSSv3 Categorization is found in the appendix of this document.

Distribution of Pentest Finding Severity

The following finding severity distribution is determined using CVSSv3 score categorization.

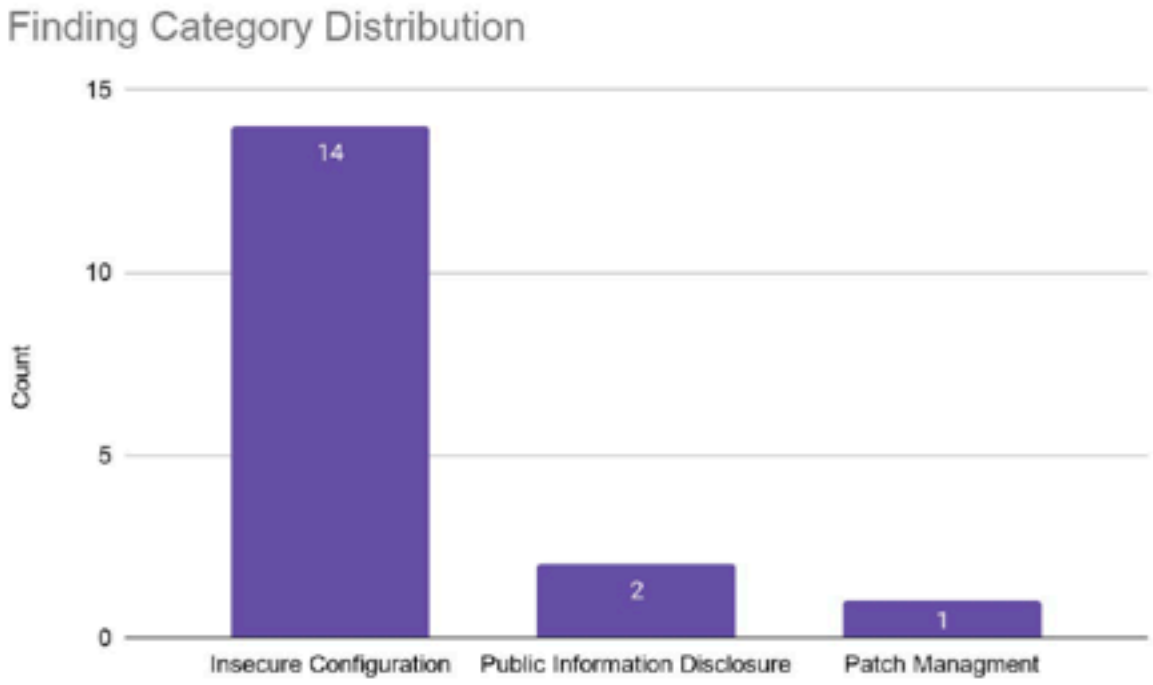


Finding Categorization

Insecure Configuration: The assessment team observed a missing configuration or incorrectly configured service that is a security risk.

Public Information Disclosure: Information pertaining to internal corporate actions and state is publicly disclosed on the internet.

Patch Management: The assessment team observed a system that lacked up-to-date patches and updates.



Critical Risk Findings

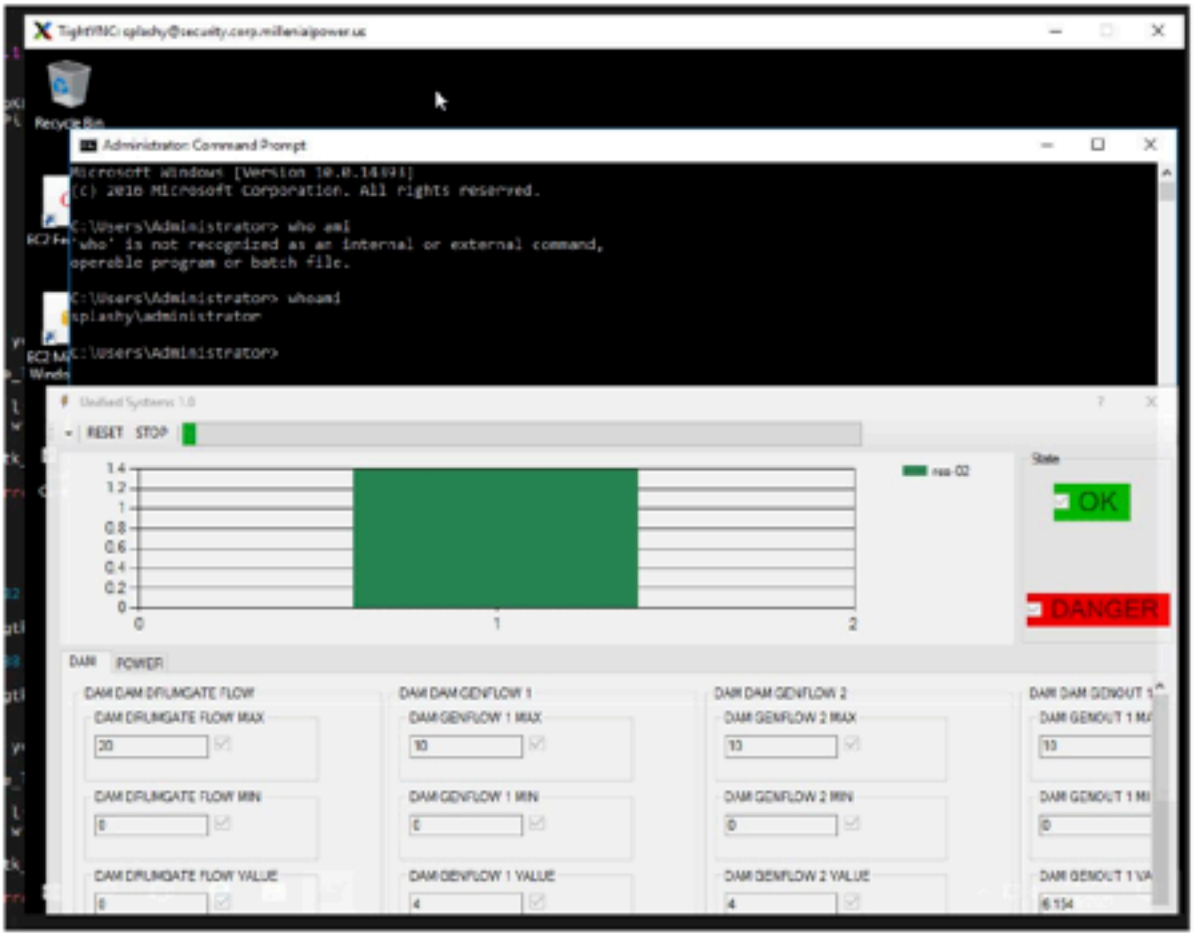
NGPEW-FINAL-01: *Unauthenticated VNC Server on Operational Technology Dashboard*

Threat Level: Critical (9.9)[5]

Category: Insecure Configuration

Description:

A Virtual Network Computing (VNC) Server is listening on the Windows server host used to monitor the NGPEW power system. The VNC session opens with user "Administrator" and shows a "Unified Systems" dashboard. This dashboard is able to view information such as dam flow, generator flow, power output, and the current state of the system. Also included is a "RESET" and "STOP" button, however the assessment team did not test if these worked in order to ensure the safety and security of personnel surrounding the system as well as the integrity of the system as a whole.



Desktop after connecting to host with VNC

[5] CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Business Impact:

Given the high level of access an unauthenticated user has with this dashboard and system, this is a critical risk to the operation of NGPEW's power and dam systems. In addition, this could be interpreted as a violation of CIP-005-6 part 2.3 requiring "Multi-factor authentication for all interactive remote access sessions" related to High and Medium impact BES Cyber Systems. In this case, no authentication is necessary.

Affected Asset(s):

`10.0.5.50`

Reproduction Steps:

Connect to the host using a standard VNC client with no authentication settings.

Remediation:

Authentication should be implemented for the VNC server on the affected host. If possible, implementing security authentication features such as Multi-Factor Authentication (MFA) is recommended to ensure further security. Remediation of this issue would support the Executive Recommendation of centralized authentication and authorization by backing authentication with a central source such as the NGPEW domain.

High Risk Findings

NGPEW-FINAL-02: *Java Web app debugging tools in production*

Threat Level: High (8.9)[6]

Category: Insecure Configuration

Description:

Java Debug wire Protocol and Java RMI are listening for remote connections on `10.0.5.75` and are attached to running applications. These are debug tools for Java web applications and are not built for use in production due to a lack of authentication as well as their capabilities to modify execution of the program on the server. Debugging tools can be used to access private and confidential information as it is processed by the target application without adhering to any authorization standard, thus allowing complete access to the application.

```
8000/tcp  open   java-rmi   Java RMI
| rmi-dumpregistry:
|   jmxrmi
|    implements javax.management.remote.rmi.RMIServer,
|    extends
|    java.lang.reflect.Proxy
|    fields
|          Ljava/lang/reflect/InvocationHandler; h
|          java.rmi.server.RemoteObjectInvocationHandler
|          @localhost:8000
|          extends
|_              java.rmi.server.RemoteObject
12345/tcp open   jdwp       Java Debug Wire Protocol (Reference Implementation)
version 1.8 1.8.0_252
```

NMAP scan including script output for Java debugging tools on KillBill Server

Business Impact:

Excessive information from the debug console could be used to access sensitive application-specific information.

Affected Asset:

`10.0.5.75 - KillBill Server`

[6] CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:L

Reproduction Steps:

Connect to the KillBill server using nmap with the following command. If the program is listening the result will be contained in the results of the scan.

```
$ nmap -Pn -A -p 12345,8000 10.0.5.75
```

Remediation:

If possible, disable Java RMI by not using it in code deployed on the server. If this is not possible, consider blocking access to the services by enforcing a strict access control policy via firewalls or AWS EC2 Security Groups.

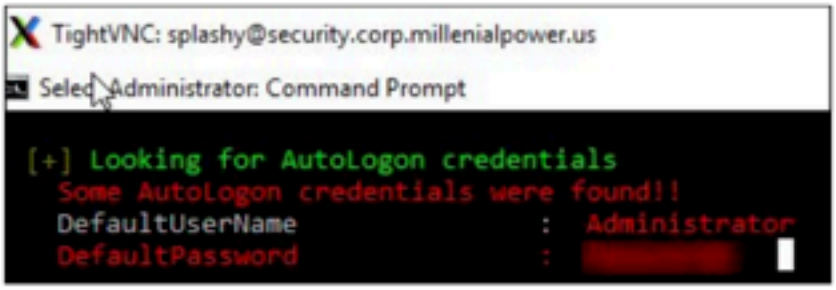
NGPEW-FINAL-03: *Autologon Credential of low quality found on Splashy*

Threat Level: High (8.8)[7]

Category: Insecure Configuration

Description:

The user `Administrator` on Splashy is configured to login automatically on system start. In order to automatically log into the user account, Windows stores the user's credentials in plaintext. While scanning Splashy with Winpeas, the privileged account `Administrator`'s password was visible. This password was notably weak, using a commonly guessed string and a number. This configuration allows any user with access to the machine's console to automatically logon as the local `Administrator`.



Administrator's Login Credentials found by Winpeas

Business Impact:

Access to this credential would allow a user access to the Administrator account of Splashy's Dam control dashboard. The dam control dashboard is a critical asset which allows users to modify the operation of NGPEW's dam system, possibly leading to loss of life and financial damages.

Affected Asset(s):

`10.0.5.50 - SPLASHY`

Reproduction Steps:

Execute the following command on SPLASHY

```
Get-ItemPropery -Path "Registry::HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\DefaultPassword"
-Name "DefaultPassword"
```

`PowerShell command used to access Autologon credentials`

[7] CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Remediation:

1. Replace the Administrator password on SPLASHY with a strong password containing at least 8 characters, a mix of capital and lowercase alphanumerics, and symbols with no commonly used or easily guessed substrings.
2. Remove autologon configuration from SPLASHY. If this is not possible, change the user which is automatically logged on to a less privileged user than the local Administrator, such as a `dashboard` user.

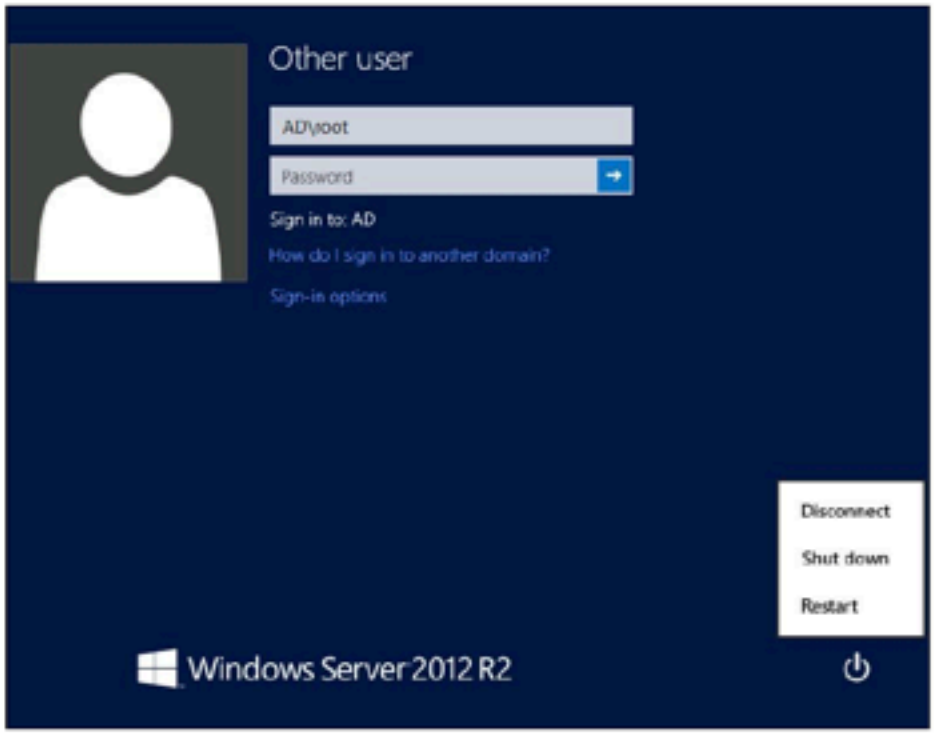
NGPEW-FINAL-04: *Can shutdown AD from unauthenticated RDP session*

Threat Level: High(8.6)[8]

Category: Insecure Configuration

Description:

Unauthenticated users have permissions to connect to the domain controller and shutdown or restart the host. This would cause the services hosted by the domain controller to be offline until the server completes a restart or there is manual intervention to initiate a power on.



Screenshot taken directly after connecting via RDP prior to authentication

Business Impact:

Business services provided by the domain controller can be unexpectedly rendered inaccessible for a period of time. Employee workstations using this server to authenticate may experience authentication issues and inability to use their workstations. This could also be in violation of CIP-007-6 part 5.1: "Have a method(s) to enforce authentication of interactive user access, where technically feasible", as an attacker is able to interact with the host (an applicable Electronic Access Control or Monitoring System EACMS).

[8] CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

Affected Asset(s):

`10.0.1.100 - ad.corp.millenialpower.us`

Reproduction Steps:

From the Windows login screen, locate the power button in the lower right corner. After clicking that option you are presented with power options, and can shut down or restart the machine from there. The presence of the button alone means a remediation is not applied.

Remediation:

Change the “Shutdown: Allow system to be shut down without having to log on” Group Policy setting to be “disabled.” This would prevent the power options from appearing on the lock screen. A related document from Microsoft[9] also details information related to remediation of the issue as well as default values.

---

9 https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/shutdown-allow-system-to-be-shut-down-without-having-to-log-on

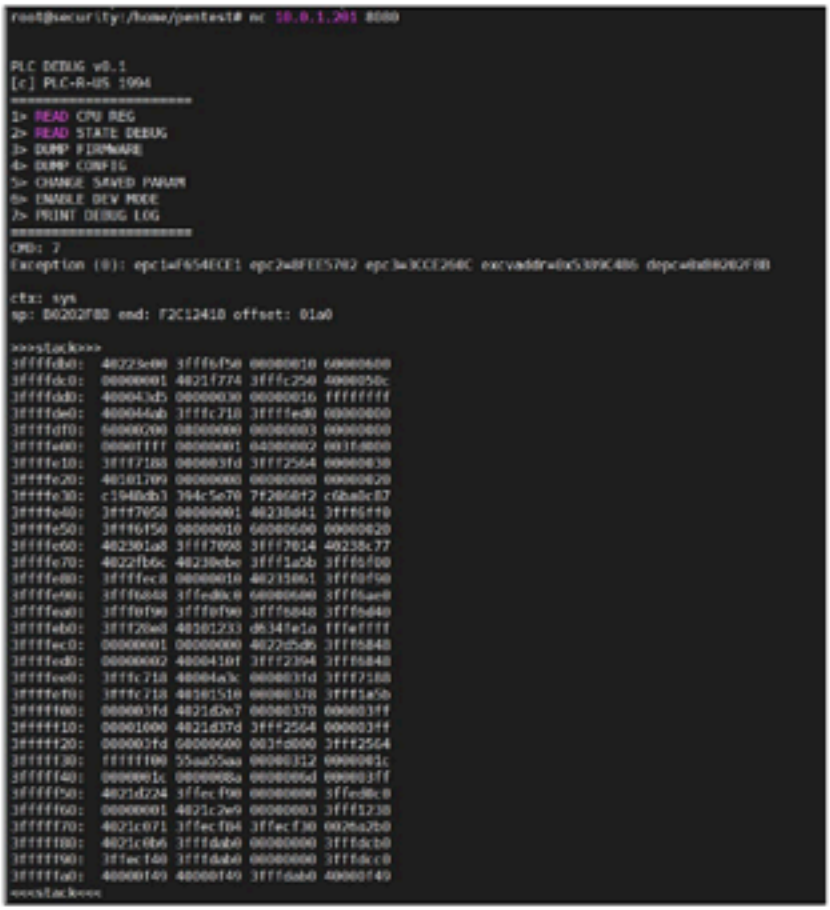
NGPEW-FINAL-05: *PLC Debug Exposed to Internal Networks*

Threat Level: High(8.5)[10]

Category: Insecure Configuration

Description:

Debug systems for PLC systems running ModBus are accessible from the corporate network. As such, an unauthorized user on the corporate network is able to modify PLC systems on the operational technology network.



Accessing Debug Logs on a PLC System

Business Impact:

Unauthorized users are able to modify the state of PLC systems as well as dump firmware information. This could be in violation of CIP-005-6 Part 2.3 requiring "multi-factor authentication for all interactive remote access sessions"

[10] CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

Affected Asset(s):

10.0.1.200
10.0.1.201
10.0.1.203

Reproduction Steps:

Run the following command from the provisioned security scanner server at 10.0.1.50:

```
$ nc 10.0.1.201 8080
```

Remediation:

PLC network assets should not be accessible from the corporate network. It is recommended to air gap this network or otherwise isolate it from the rest of the network as per the executive recommendation "Improve Network Segmentation"

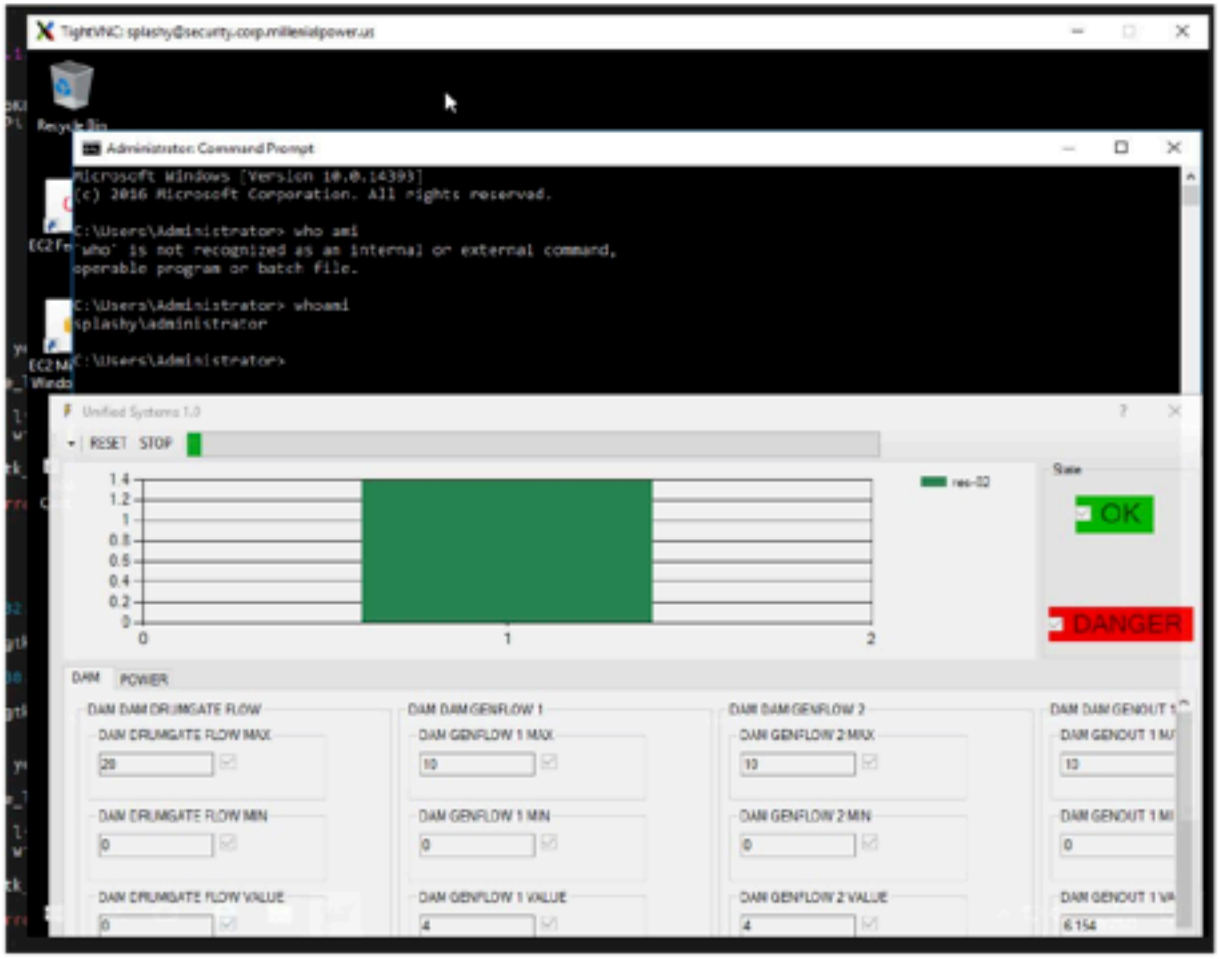
NGPEW-FINAL-06: *Operational Technology System Dashboard Running as Administrator*

Threat Level: **High (8.2)**[11]

Category: Insecure Configuration

Description:

When connected via VNC to the System Dashboard, the current user is the privileged user `Administrator`. As a result, the Operational Technology System Dashboard is running as the local administrative user.



Command Prompt showing that the current user is Administrator

Business Impact:

[11] CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

The default user when connecting with VNC has local Administrator permissions. This grants the default user the ability to install unnecessary software, create new users, and remove critical software from the system. The current user is also able to view confidential logs and login information for other users which may connect to the system.

Affected Asset(s):

`10.0.1.150`

Reproduction Steps:

Same as NGPEW-01: Connect to the host using a standard VNC client with no authentication settings. It is recommended that TightVNC is used as it was used in our testing.

Remediation:

Create a new, lower privilege user account for the dashboard application. This user should only be able to use the necessary programs and make the required changes to the system that the dashboard needs to function. This could be a new user in the NGPEW domain in support of the Centralized Authentication and Authorization executive recommendation.

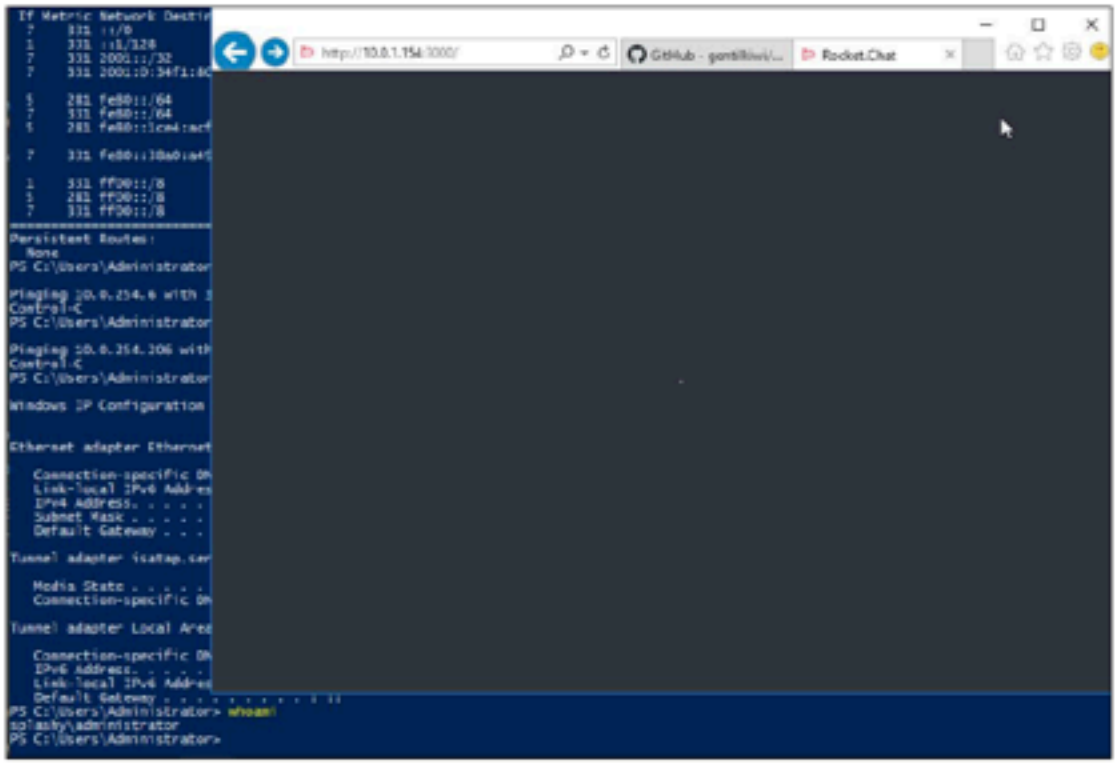
NGPEW-FINAL-07: *AWS Security Groups Allow Access to Non-essential Assets*

Threat Level: **High(7.7)**[12]

Category: Insecure Configuration

Description:

The host SPLASHY is able to access NGPEW's primary Rocket.Chat server. Given that this access is not thought to be necessary, security policies should be implemented to restrict SPLASHY's access to corporate chat servers. In addition, SPLASHY is able to access internet resources such as GitHub allowing attackers to download tools for further exploitation. Configuring AWS security group policies per host to only allow necessary access is critical to securing a cloud deployment.



SPLASHY receiving data back from Rocket.Chat server

It was found that other machines on the network running services not critical to SPLASHY's use case were accessible from the host, such as the company communications platform, Rocket.Chat.

[12] CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:L/A:L

Business Impact:

By utilizing SPLASHY's non-minimal egress access, an attacker or unauthorized user can access core NGPEW assets. This could also violate CIP-005-6 Part 1.3 requiring "inbound and outbound access permissions".

Affected Asset(s):

SPLASHY and NGPEW AWS VPCs

Reproduction Steps:

Reproduction steps are not applicable to this finding.

Remediation:

Reconfigure AWS Security Groups and Network Policies to only allow minimal ingress and egress from the host. To do this in AWS, we recommend configuring per-host security policies. A useful resource for this is the AWS official documentation[13].

[13] https://docs.aws.amazon.com/cli/latest/userguide/cli-services-ec2-sg.html

Medium Risk Findings

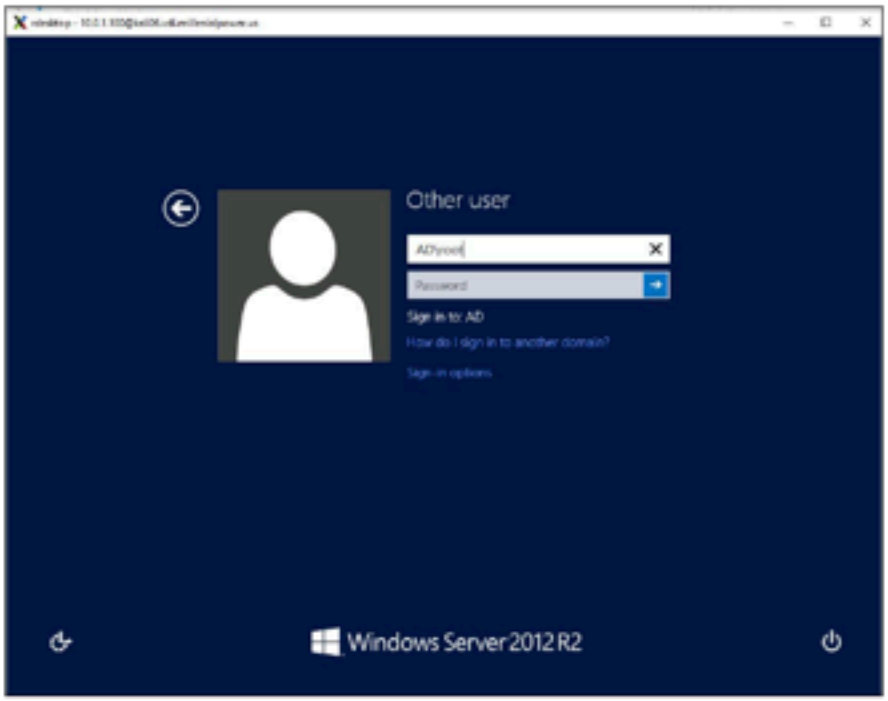
NGPEW-FINAL-08: *RDP Network-Level Authentication Not Required*

Threat Level: Medium (5.8)[14]

Category: Insecure Configuration

Description:

Network Level Authentication is a security setting for RDP that requires clients to use a more secure method of connecting. By having this disabled, less secure clients are able to connect to the Remote Desktop Server. Additionally, Remote Desktop Connections are allowed to connect without first authenticating. This presents clients with the Windows login screen where information disclosure is possible, such as currently logged in users. Together with finding ***NGPEW-FINAL-03***, the host server can be powered off.



RDP Session created prior to user authentication

Business Impact:

An unauthenticated user is able to view the previously logged in AD account username, which could disclose the account name of possible systems administrators. In this case, the user is also able to act on the target machine by powering off the server as detailed in ***NGPEW-FINAL-03***.

[14] CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N

Affected Asset(s):

`10.0.1.100 - ad.corp.millenialpower.us`

Reproduction Steps:

Run the following command to see the machine's current NLA configuration:

```
(Get-WmiObject -class "Win32_TSGeneralSetting" -Namespace root\cimv2\terminalservices -Filter
"TerminalName='RDP-tcp'").UserAuthenticationRequired
```

PowerShell Command to Check if NLA is Enabled

A user could also use RDP to connect to the machine and validate that the user will not need to authenticate prior to the creation of a session.

Remediation:

It is highly recommended that NLA is enabled. To enable NLA, run the following command on the Domain Controller:

```
(Get-WmiObject -class Win32_TSGeneralSetting -Namespace root\cimv2\terminalservices -Filter
"TerminalName='RDP-tcp'").SetUserAuthenticationRequired(1)
```

PowerShell Command to Enable NLA

NGPEW-FINAL-09: *Power Management API Has No Authentication*

Threat Level: **Medium (5.3)**[15]

Category: Insecure Configuration

Description:

An exposed API endpoint for NGPEW's power management system exposes data about the current status of the system without authentication. The assessment team was able to view metrics such as Dam flow, power output, and other values. Given that this system appears sensitive to manipulation, there was no further tampering performed so as to avoid physical damage and to ensure the safety of workers around the system.

API Information Viewable

[15] CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Business Impact:

Information disclosed by this API could pose potential risk to the business due to a lack of confidentiality and integrity. Performance information about NGPEW power systems should not be available without authentication.

Affected Asset(s):

`https://10.0.10.15:80/`

Reproduction Steps:

Access the affected asset in a web browser.

Remediation:

Implement some form of authentication to ensure that sensitive information is not available to unauthenticated users. Examples of possible authentication systems include Okta, Duo, Azure Cloud AD, or another key provisioning system.

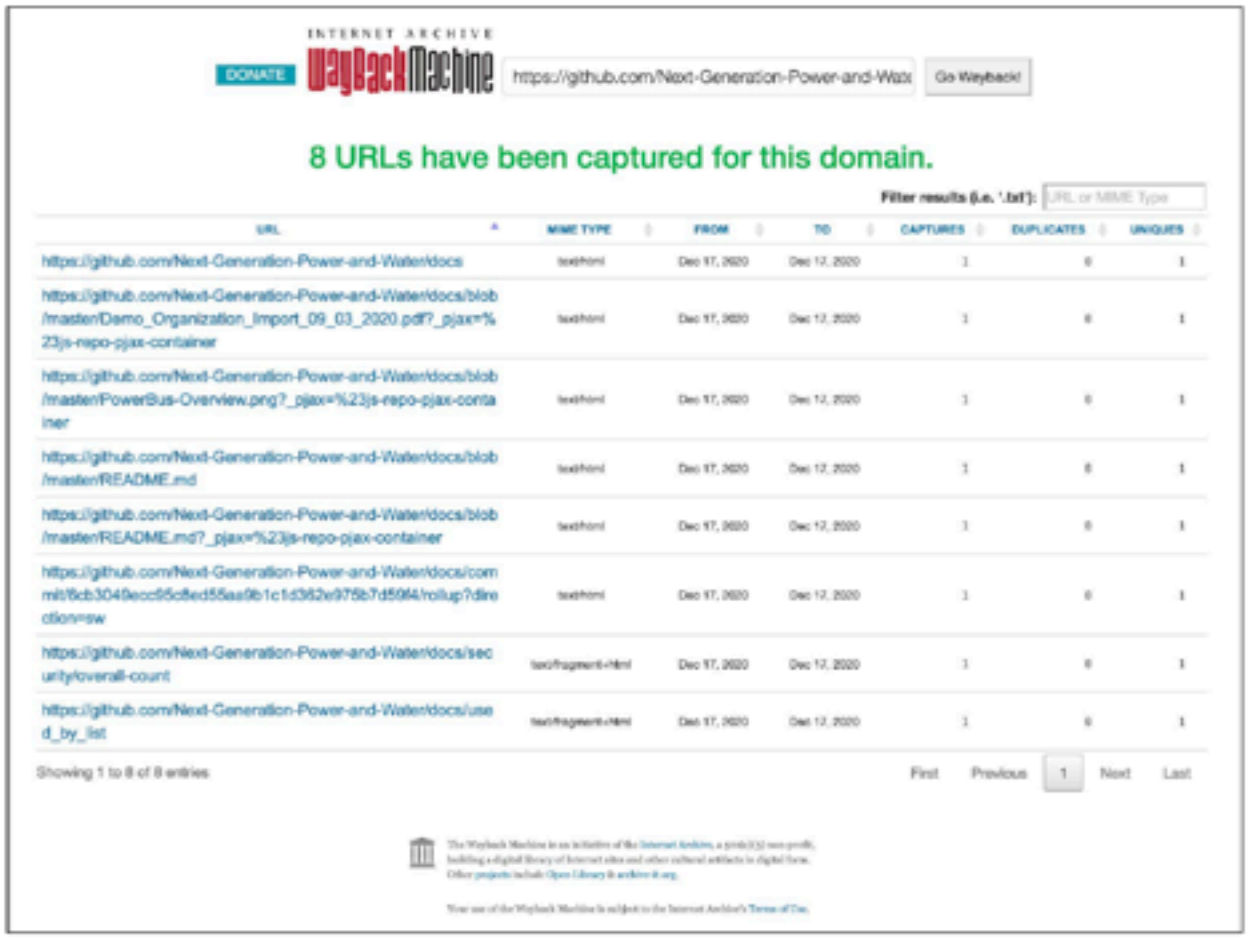
NGPEW-FINAL-10: *Public Github Repository of Internal Documents*

Threat Level: **Medium (5.3)**[16]

Category: Inadequate User Practice

Update from October Assessment:

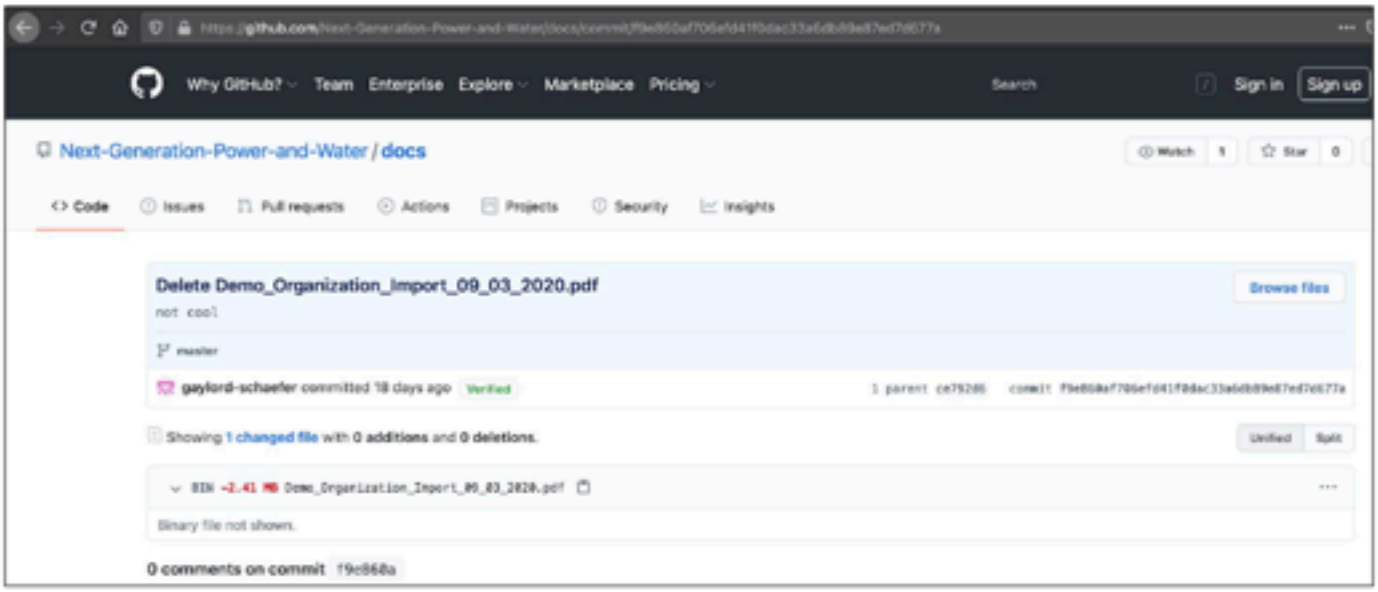
Since the October assessment, user gaylord-schaefer on GitHub has added two commits deleting the sensitive documents that were previously discovered. Deleting files via git commits will not remove the files from the public internet and since that time the files are still visible when viewing the repository's git commit history. Our recommended remediation steps are still recommended, although internet archival projects such as The Wayback Machine[17].



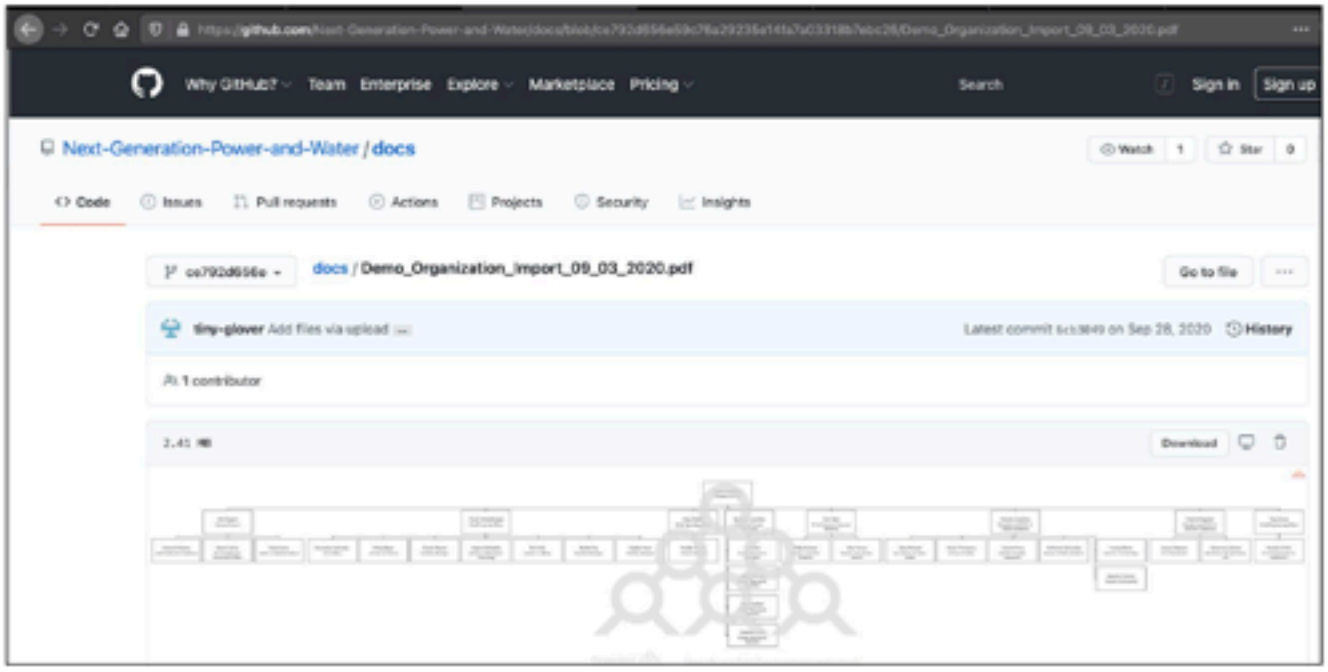
NGPEW Documents found on the Wayback Machine

[16] CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

[17] https://web.archive.org/web/*/https://github.com/Next-Generation-Power-and-Water*



Commit deleting organization chart from GitHub repository



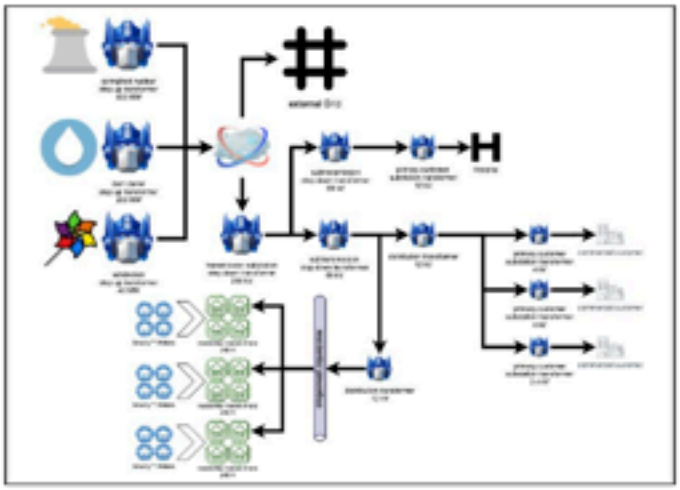
PDF Visible in the Github repository as of January 9th, 2021

Description:

NGPEW's employee organization chart was originally posted in a public Github repository named "docs" under their official GitHub account and has since been deleted. Though by going through the repository's

commit section[18] it is still possible to view these files. This is information disclosure about the internal structure of the company providing attackers with information that can facilitate social engineering attacks against the company. Furthermore, there is also a PDF file that contains a chart containing PowerBus information.

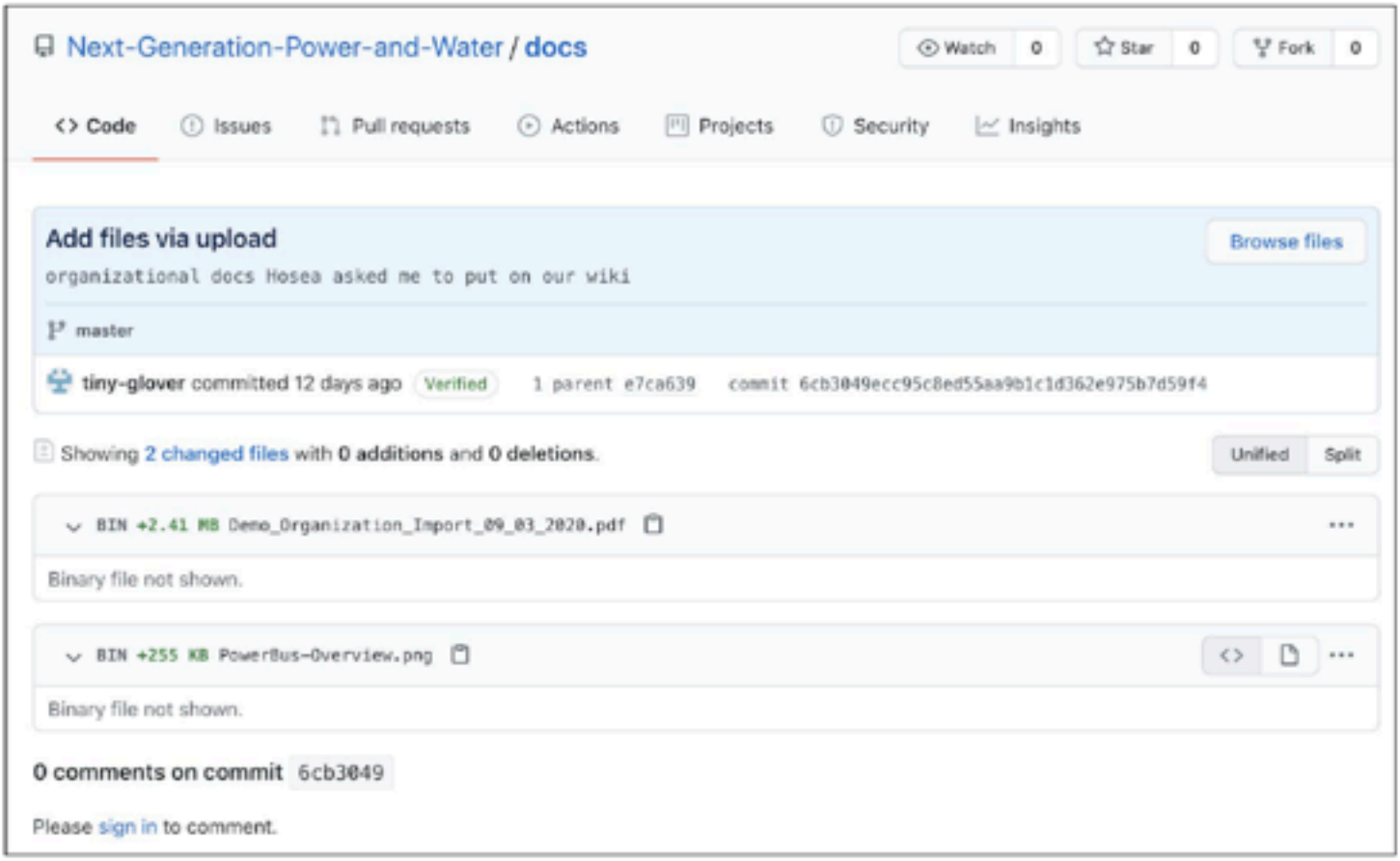
Organization chart posted in GitHub



PowerBus Overview posted in GitHub

18

https://github.com/Next-Generation-Power-and-Water/docs/blob/ce792d656e59c76a29235e14fa7a03318b7ebc26/Demo_Organization_Import_09_03_2020.pdf



Initial Commit of the two files

Business Impact:

By not properly deleting the files off the public GitHub account, the files are still obtainable. Having these documents open in a public github repository is information disclosure that presents risks to the organization. The employee organization chart shows the names of employees which is information that can be used in social engineering campaigns.

Affected Asset(s):

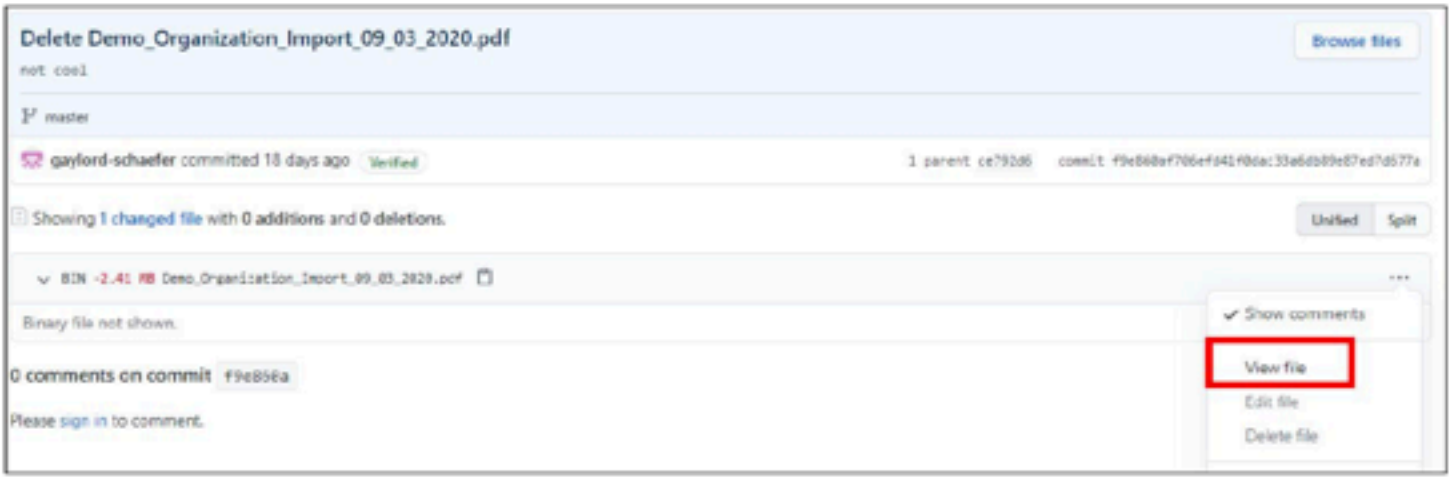
N/A

Reproduction Steps:

Going to the NGPEW documentation github repository[19] anyone can view the "docs" repository which used to contain the two PDF files - the employee organization chart and the PowerBus Overview. However, since the files were not deleted properly, anyone can still view them by first viewing the commit

[19] https://github.com/Next-Generation-Power-and-Water/docs

history by clicking on the number of commits near the top right next to the clock. Click on the commit that involves deleting the wanted file. Click the three dots to the right of the file name and click *View file*.



Viewing the deleted organizational chart

Remediation:

Make the currently public repository private. This can be done by first navigating to the repository and clicking the *Settings* option near the top left next to the gear icon. Aftwards, scroll all the way down and under *Danger Zone* there is a *Change visibility* button which will give you the option to *Make private*. Click that option and confirm by typing in the repository name would make the repository private. Creating a private repository that only employees within the organization can access or uploading the chart to an internal website would ensure that the employee organization chart is not publicly available.

NGPEW-FINAL-11: *SMB Signing Not Required*

Threat Level: **Medium (5.3)**[20]

Category: Insecure Configuration

Description:

Message Signing is not required on the remote Server Message Block (SMB) server. An unauthenticated, remote attacker can exploit this to conduct session hijacking and man-in-the-middle attacks against the SMB server.[21]

```
|   FQDN: splashy.corp.millenialpower.us
|_  System time: 2020-10-10T13:20:49+00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2020-10-10T13:20:47
|_  start_date: 2020-10-09T21:15:36
```

Nmap scan results showing SMB message signing as "not required"

Business Impact:

It allows for man-in-the-middle attacks which puts the confidentiality of the system at risk. It can potentially result in the leaking of sensitive business information.

[20] CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

[21] https://www.tenable.com/plugins/nessus/57608

Affected Asset(s):

```
10.0.1.10 grace.corp.millenialpower.us
10.0.1.11 gaylord.corp.millenialpower.us
10.0.1.12 tiny.corp.millenialpower.us
10.0.1.13 porfirio.corp.millenialpower.us
10.0.5.50 SPLASHY
```

Reproduction Steps:

Execute the following command to check for current SMB information:

```
nmap -script smb-check-vulns.nse -script-args=unsafe=1-p445 [host]
```

Remediation:

SMB signing allows the recipient of SMB packets to confirm their authenticity. It provides a way to ensure that the client is receiving genuine Group Policy. SMB signing should be configured to be enabled and required. Additionally SMBv1 can be disabled on the host by using the add or remove windows features control panel.

To enable SMB signing, set the following registry key value to 1 then restart the server:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\Ena
bleSecuritySignature
```

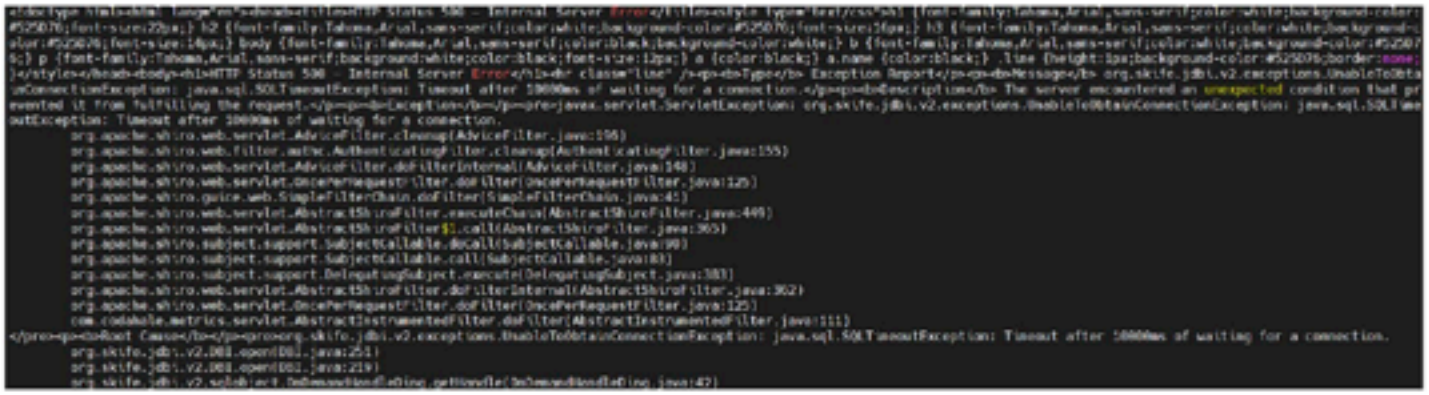
NGPEW-FINAL-12: *Internal Server Error Information Disclosure on KillBill API*

Threat Level: Medium (5)[22]

Category: Insecure Configuration

Description:

The KillBill API server exposes Java stack traces upon database timeout errors. Details of database errors could contain critical information such as credentials and internal implementation details to the KillBill system. In our assessment, no critical information was found in the returned stack trace, however this message does provide excessive information about the configuration of KillBill



Java error disclosure found on the KillBill API

Business Impact:

An attacker could use the information in an error message to further develop an attack and/or receive privileged information as well as details pertinent to the implementation of the KillBill API. An attacker is also able to determine whether or not a request times out upon querying the application's database, allowing development of a DDoS program.

Affected Asset(s):

`10.0.5.75 - KillBill Server`

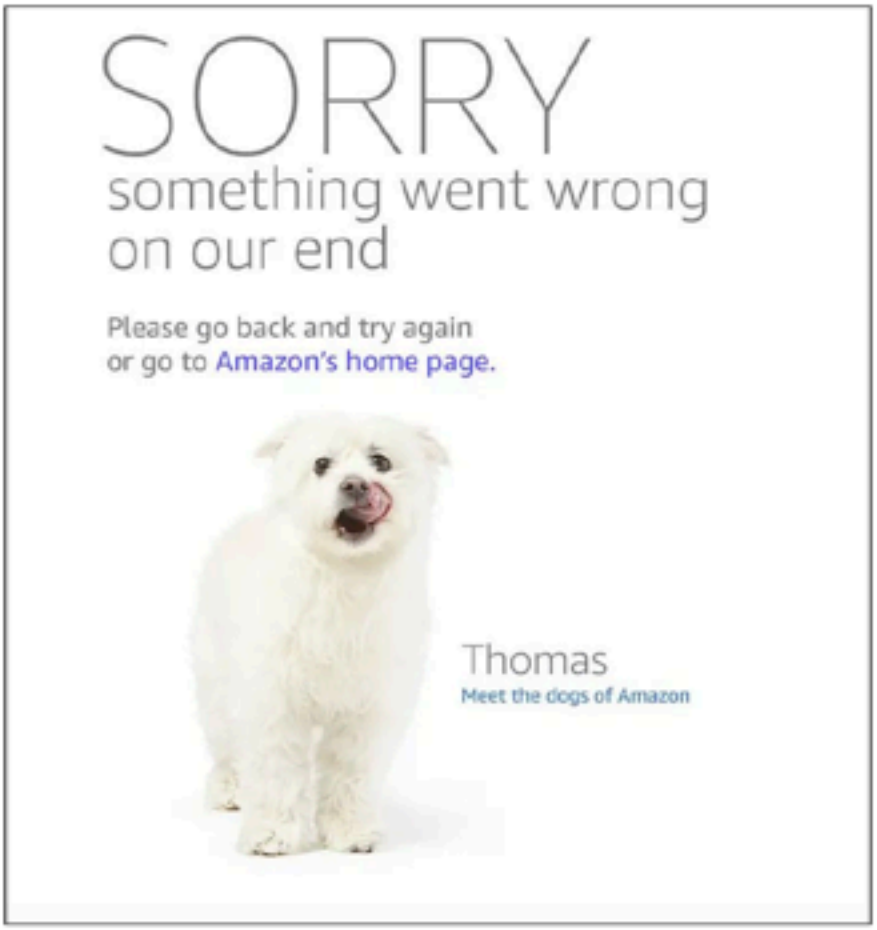
Reproduction Steps:

Producing many requests will overload the KillBill server, resulting in a stack trace to be returned.

[22] CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N

Remediation:

In order to provide minimal information about a server error, implement a standard error page which does not contain the stack trace of the application. Guides exist for implementing this with tools such as NGINX[23], however given that this application is running on Apache Tomcat, there are guides for implementing similar standard error pages relevant to Apache Tomcat[24].



Amazon uses pictures of Dogs for their custom error pages

[23] https://www.digitalocean.com/community/tutorials/how-to-configure-nginx-to-use-custom-error-pages-on-ubuntu-14-04

[24] https://www.yeahhub.com/set-custom-error-page-apache-tomcat-server/

Low Risk Findings

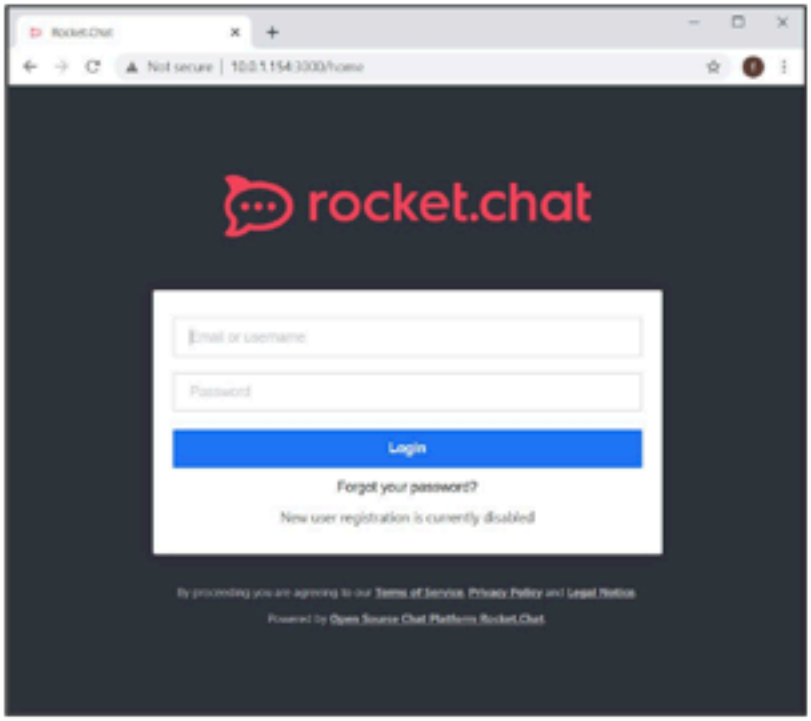
NGPEW-FINAL-13: *Lack of TLS/SSL Encryption on Multiple Applications*

Threat Level: Low (2.9)[25]

Category: Insecure Configuration

Description:

TLS/SSL encryption secures communication between client and server communications. This encryption protects the information being transmitted from unwanted eavesdropping. For some applications the implementation of this protocol may be necessary for some features of the application to function properly.



The Rocket.Chat instance only allows use with HTTP with no encryption

Business Impact:

The implementation of TLS/SSL encryption will secure business communication so t
hat the integrity and confidentiality of business data is preserved.

Affected Asset(s):

[25] CVSS:3.0/AV:P/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N

```
10.0.1.154 Rocket.Chat server
10.0.1.152 ngpew.com
```

Reproduction Steps:

Reproduction steps are not applicable to this finding.

Remediation:

Implement TLS/SSL encryption for HTTP-based services. In the case of Rocket.Chat, it is recommended that the server not listen on port 3000 externally, but rather listen on 127.0.0.1:3000 with a secure web reverse proxy such as Nginx or Apache, encrypting incoming traffic with a TLS certificate and redirecting traffic to the internal web server. An example of this process can be found in the Rocket.Chat official documentation[26].

[26] https://docs.rocket.chat/installation/manual-installation/configuring-ssl-reverse-proxy

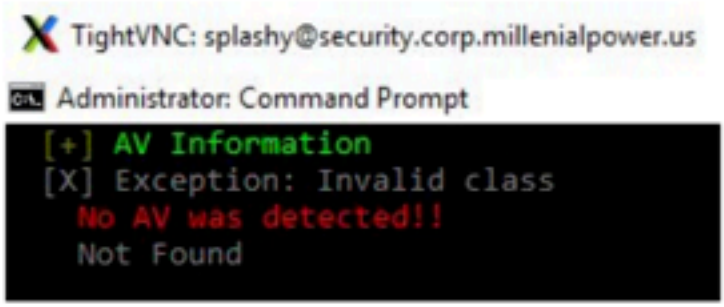
NGPEW-FINAL-14: *No Antivirus or Antimalware Systems in Place*

Threat Level: Low (3.9)[27]

Category: Insecure Configuration

Description:

Antivirus and Antimalware software automatically detect and remediate malicious content. There is an absence of both of these protections in the corporate environment which may place the computer systems at risk. By allowing malicious software to be placed on the machine without automatic removal, additional exploits may be possible. During the assessment malicious pieces of code was able to be downloaded for the assessment without any form of detection or removal.



Business Impact:

The absence of software to automatically detect and remove malicious software puts the integrity of the computer systems at risk. Software can be placed on the machine that may interfere with general business activities. This finding could indicate non-compliance with CIP-007-6 Part 3.1

Affected Asset(s):

ALL

Reproduction Steps:

N/A

[27] "CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Remediation:

Install and configure antivirus, antimalware, or other endpoint detection and response (EDR) software. Consider implementing QRadar[28] event management tool.

[28] https://www.ibm.com/products/qradar-siem

Informational Findings

NGPEW-FINAL-15: *End of Life Windows System Versions*

Description:

Within the NGPEW network, there are hosts running versions of Windows operating systems that are no longer supported by the developers and have been declared End of Life (EOL). Windows operating systems declared EOL no longer receive security updates or other regular patching services from Microsoft. Extended support licenses are available for EOL operating systems for a limited time period at a varying cost. Extended support for Windows Server 2000 and 2008 ended permanently on January 14th, 2020. Mainstream support for Windows Server 2012 ended on October 9th, 2018 and extended support will be ending on January 10th, 2023. When vulnerabilities are found on EOL systems, there will not be any updates that are pushed out which create a risk to the network.

All releases

Release	Release date	End of life	Extended Support
Windows Server 2019 Datacenter	November 13, 2018	January 9, 2024	January 9, 2029
Windows Server 2019 Essentials	November 13, 2018	January 9, 2024	January 9, 2029
Windows Server 2019 Standard	November 13, 2018	January 9, 2024	January 9, 2029
Windows Server 2016 Datacenter	October 15, 2016	January 11, 2022	January 11, 2027
Windows Server 2016 Essentials	October 15, 2016	January 11, 2022	January 11, 2027
Windows Server 2016 Standard	October 15, 2016	January 11, 2022	January 11, 2027
Windows Server 2012 Standard	October 30, 2012	October 9, 2018	October 10, 2023
Windows Server 2012 Datacenter	October 30, 2012	October 9, 2018	October 10, 2023
Windows Server 2008 Small Business Server Standard	November 21, 2008		January 14, 2020
Windows Server 2000 Datacenter Server	November 13, 2000	June 30, 2005	July 13, 2010
Windows Server 2000 Server	March 31, 2000	June 30, 2005	July 13, 2010

https://endoflife.software/operating-systems/windows/windows-server

Business Impact:

Having end of life systems within the network presents a security risk for the organization. Due to Microsoft no longer providing updates to these operating systems, these systems will no longer have updates that include security fixes meaning that vulnerabilities that are discovered won't be patched: creating a security hazard within the network. In addition, having old operating systems can present

compatibility issues when adding newer applications to the environment. EOL systems also are likely to have legacy applications which present further risks.

Affected Asset(s):

`10.0.5.152 - NGPEW.com`

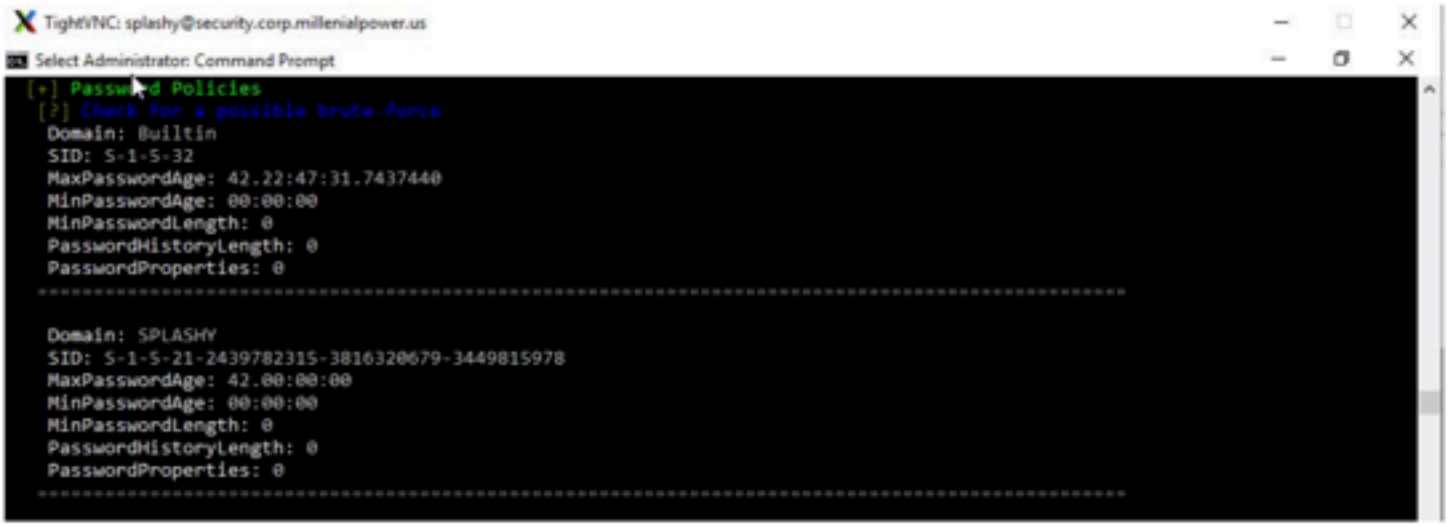
Remediation:

Design and implement an Operating System patch management cycle which allows for ample time to upgrade and patch systems as necessary. Other remediation could include segmenting machines which are unable to be patched in a timely manner from the rest of the network.

NGPEW-FINAL-16: *Weak Windows Password Policy*

Description:

It was discovered that NGPEW's password policy does not include a minimum password length or a minimum password age. This does not follow best security practice in regards to password policies thus presenting a risk to the environment.



Screenshot showing there's no set minimum password length and age

Business Impact:

Having weak password policies presents a risk to the corporate environment. Attackers can brute-force, crack, or guess weaker passwords to gain unauthorized access to NGPEW's internal network which would compromise the integrity of the affected systems. Having a strong password policy is also necessary to keep the confidentiality of all information within the network intact.

Recommendation:

It is our recommendation that password policy match industry-standard complexity requirements as defined in the official Microsoft documentation[29].

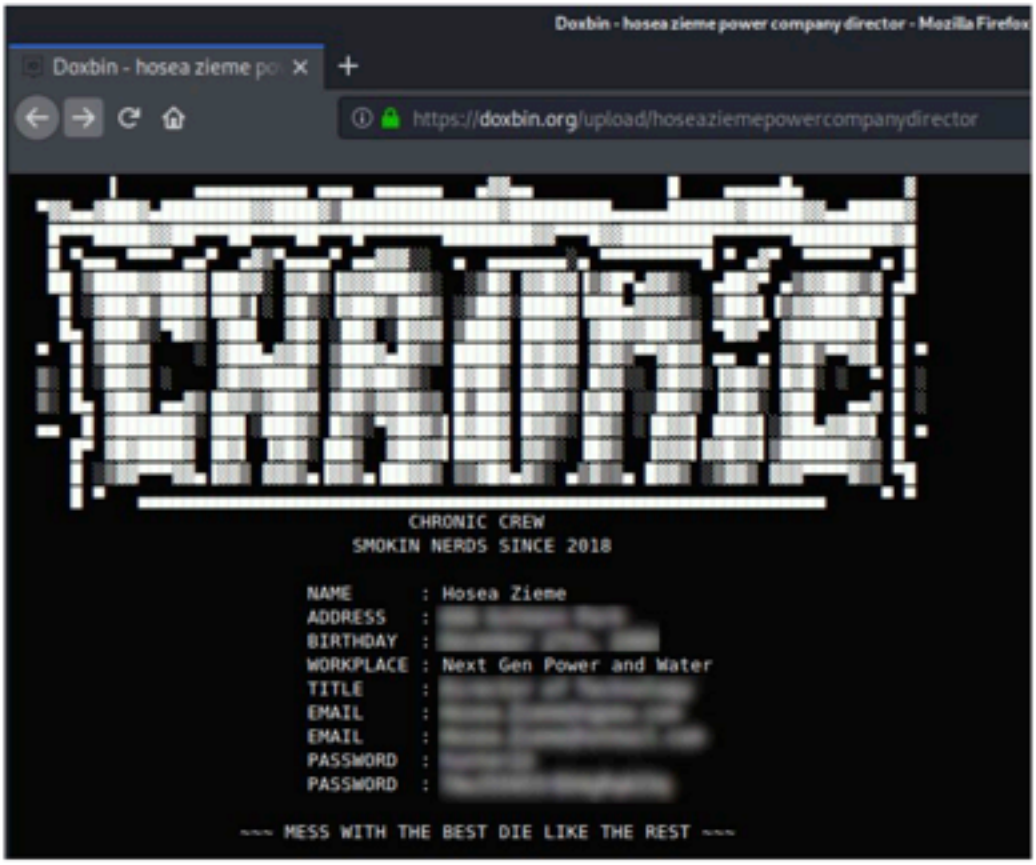
29

https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-must-meet-complexity-requirements

NGPEW-FINAL-17: *Exposed Employee Data (OSINT)*

Description:

Using open source intelligence (OSINT) techniques, an employee's NGPEW email and password was obtained. Only one employee's email address and password was found to be publicly available. Though in addition to their work credentials, other personally identifiable information (PII) was also dumped which includes address, birthday, and a personal email address with its corresponding password.



Doxbin post containing employee credentials and information

Business Impact:

These credentials belong to the Director of Technology, making it a high valued account. Attackers who discover this information can utilize these credentials as an initial access point to gather more information about the company. Furthermore, this also exposes the email syntax for company email accounts, giving the attackers a lead to start social engineering attempts on all other staff using a similar format of `FirstName.LastName@ngpew.com`. It is worth noting that during the second pentesting

engagement, these credentials were attempted throughout the environment and did not result in any valid logins.

Conclusion

Overall, Next Generation Power and Water applications tested to be well designed and to be utilizing many solid security practices. NGPEW can pride itself on its dedication to industry standards and best security practices. During testing, it was noted that modern software such as Splunk was used to monitor incoming logs and metrics alongside enforcement of elementary security fundamentals demonstrate the considerable security posture of NGPEW. The addition of new security isolation techniques such as network ACL policies improved NGPEW's network posture significantly.

Mediating the vulnerabilities discovered and reported in the Technical Briefings section of this assessment can further strengthen the NGPEW's security. It is strongly advised that NGPEW incorporate the remediations for the reported vulnerabilities as described in the Executive Recommendations' section, as well as each individual finding's remediations to ensure the reliability and safety of their critical infrastructures and services. A defensive security posture is strengthened by active harm mitigation. Upon following the suggested recommendations, NGPEW will maintain confidentiality, integrity, and availability of its critical infrastructures.

Appendix

Artifacts

These are the things left behind in the environment because of the inability to remove them at the conclusion of the engagement:

Artifact	Location
Folder `C:\Users\hacker`	SPLASHY

Resolved and Unconfirmed Findings

Finding ID and Name	Status
NGPEW-02: Domain Administrator Credential In Rocket.Chat	Circumstantial finding in previous assessment. No repeat finding.
NGPEW-03: User Credentials Stored in Description Property	Unable to validate
NGPEW-06: Mantis Ticketing System Unauthenticated Remote Code Execution	Resolved (Application no longer exists)
NGPEW-07: Rocket.Chat Stored Cross-Site Scripting	Unable to validate version due to NGPEW-10 remediation
NGPEW-08: PowerShell Remoting Enabled for Machine Accounts	Unable to validate
NGPEW-09: No Detection for Named Pipe Privilege Escalation	Unable to validate
NGPEW-10: Rocket.Chat Unauthenticated User Creation	Resolved
NGPEW-11: Unauthenticated thinVNC Client	Resolved (Application no longer exists)

NGPEW-12: Mantis Ticketing System with Exposed Installation Dashboard	Resolved (Application no longer exists)
NGPEW-18: Apache Logs in Incorrect Directory	Resolved (Application no longer exists)

Network Services and ports

10.0.1.0/24 Corporate Network Hosts and Services

IP Address	Hostname	Service/Port (TCP unless specified)
10.0.1.10	GRACE	135 Windows RPC 445 SMB 3389 Remote Desktop Protocol 5985 WinRM 47001 RPC randomly allocated high TCP ports 49664 RPC randomly allocated high TCP ports 49665 RPC randomly allocated high TCP ports 49666 RPC randomly allocated high TCP ports 49667 RPC randomly allocated high TCP ports 49668 RPC randomly allocated high TCP ports 49669 RPC randomly allocated high TCP ports 49685 RPC randomly allocated high TCP ports
10.0.1.11	GAYLORD	139 135 Windows RPC 445 SMB 3389 Remote Desktop Protocol 5985 WinRM 49665 RPC randomly allocated high TCP ports 49666 RPC randomly allocated high TCP ports 49670 RPC randomly allocated high TCP ports 47001 RPC randomly allocated high TCP ports 49664 RPC randomly allocated high TCP ports 49667 RPC randomly allocated high TCP ports 49668 RPC randomly allocated high TCP ports 49678 RPC randomly allocated high TCP ports 49669 RPC randomly allocated high TCP ports

10.0.1.12	TINY	135 Windows RPC 139 Netbios SSN 445 SMB 3389 Remote Desktop Protocol 5985 WinRM 49678 RPC randomly allocated high TCP ports 49669 RPC randomly allocated high TCP ports 49668 RPC randomly allocated high TCP ports 49665 RPC randomly allocated high TCP ports
10.0.1.13	PORFIRIO	135 Windows RPC 139 Netbios SSN 445 SMB 3389 Remote Desktop Protocol 5985 WinRM 49670 RPC randomly allocated high TCP ports 49666 RPC randomly allocated high TCP ports 49665 RPC randomly allocated high TCP ports 47001 RPC randomly allocated high TCP ports
10.0.1.50	Unknown	No ports recorded from pentest machine
10.0.1.60	Security	22 SSH
10.0.1.100	AD	53 DNS 88 Kerberos 135 Windows RPC 389 LDAP 445 SMB 464 Kerberos 3268 LDAPS 3269 LDAPS 3389 Remote Desktop Protocol 49152 RPC randomly allocated high TCP ports UDP/53 DNS UDP/123 NTP UDP/88 Kerberos
10.0.1.154	Maxwell	22 SSH 3000 HTTP (rocket chat)

10.0.1.198	Unknown	502 modbus
10.0.1.199	Unknown	502 modbus
10.0.1.200	Unknown	502 modbus
10.0.1.201	Unknown	502 modbus

10.0.5.0/24 Service Network Hosts and Services

IP Address	Hostname	Port/Service (TCP Unless Specified)
10.0.5.50	SPLASHY	135 RPC 139 netbios-ssn 445 SMB 3389 RDP 5900 VNC
10.0.5.75	Unknown	80 HTTP (KillBill) 3306 Mysql 8000 Java RMI 8080 HTTP (kaui-broken) 12345 Java Debug Wire Protocol
10.0.5.151	Unknown	22 ssh 3306 Mysql
10.0.5.152	NGPEW.com	80 HTTP (NGPEW site) 135 RPC 443 HTTPS (NGPEW site) 5900 VNC (realvnc)
10.0.5.153	support.millenialpower.us	22 SSH 80 HTTP (empty directory listing)

10.0.10.0/24 Operational Technology Network Hosts and Services

IP Address	Hostname	Port/Service (TCP Unless Specified)
10.0.10.15	Unknown	80 (Dam Api)
10.0.10.50	Unknown	503 ModBus
10.0.10.52	Unknown	503 ModBus
10.0.10.53	Unknown	503 ModBus
10.0.10.65	Unknown	503 ModBus

CVSSv3 Ratings System

CVSS v3.0 Ratings

Rank	Score	Description
Informational	0.0	Findings that do not follow security best practices.
Low	0.1-3.9	Vulnerabilities that result from general information leakage or are inconsistent with security best practices.
Medium	4.0-6.9	Vulnerabilities that are leveraged with one or multiple security issues to compromise the server/application.
High	7.0-8.9	Vulnerabilities where the client is compromised with warnings or prompts and whose exploitation could result in compromise of data.
Critical	9.0-10.0	Vulnerabilities that could allow remote code execution without user interaction or where code executes without warnings or prompts.

THIS PAGE INTENTIONALLY LEFT BLANK