NEXT GEN

Penetration Test Report

Next-Generation Power and Water

January 10, 2021 – Version 1.0

Prepared for

Next-Generation Power and Water

Prepared by

[redacted]

Table of Contents

Document Information

Confidentiality and Copyright

All information contained in this document is provided in confidence for the sole purpose of adjudication of the document and shall not be published or disclosed wholly or in part to any other party without prior permission in writing. These obligations shall not apply to information that is published or becomes known legitimately from some source other than [redacted]

Document History

Version Number	Issue Date	Issued By	Change Description
0.1	10/01/2021	Finals-3	Draft for internal review only
0.2	10/01/2021	Finals-3	Quality Assurance
1.0	10/01/2021	Finals-3	Released to client

Scope of Work

Penetration Test

Next-Generation Power and Water (NGPEW) asked [redacted] to undertake a penetration test against the internal infrastructure listed below. The testing was conducted in accordance with the standard infrastructure testing methodology which is included for reference within the appendix of this report.

Objectives

It is expected that securing vulnerabilities and reducing risks within the environment will lead to a reduction in the chance of:

- Abuse of publicly available exploits through lack of patching
- Financial loss from regulatory penalties
- Disruption of availability to business-critical systems
- Breaches of integrity through weak authorisation checks
- System compromise leading to data modification or destruction
- Information theft through poor safeguards
- Reputational loss through exploitation of any of the above vulnerabilities

Initial Information

The following information was provided to [redacted] testers prior to commencing the test:

- Access to a virtual desktop infrastructure within the NGPEW network
- Scope of IP range 10.0.1.0/24
- Scope of IP range 10.0.5.0/24
- Scope of IP range 10.0.10.0/24

Constraints and Limitations

The following constraints and limitations were encountered during testing:

- Minimising the impact to live industrial control systems meant that more aggressive tests and verification of findings were not possible in some cases
- Minimising the impact to employee PCs meant that more aggressive exploits such as EternalBlue that have a chance of impacting the availability of systems could not be utilised

Executive Summary

[redacted] carried out a penetration test of the infrastructure utilised by NGPEW between the 8th and 9th of January. Testing was carried out according to the standard methodology, as defined in the Appendix of this report.

Since the initial penetration test [redacted] completed in November, significant improvements have been made, improving the overall security posture of NGPEW. Recommendations have been implemented and vulnerable devices have been phased out, making the network more resilient to attacks. Overall, when compared to similar companies within the critical national infrastructure sector, the security posture was found to be slightly below average. Although some of the issues identified related solely to best practice configuration issues, the hosts overall were let down by issues around authentication and usage of outdated software. Due to this, the issues that were discovered were considered to be of a greater than average risk to the business.

The most significant issue identified related to insufficient access control to assets on the network, leading to potential for unauthorised users to retrieve and potentially modify sensitive company data. Business risk associated with this issue would include the possibility of organisation compromise and the destruction of data; affecting business continuity and leading to associated costs to remediate. Further risks might include a loss of customer confidence in the NGPEW brand in addition to civil or regulatory penalties brought by affected parties and loss of life due to critical utilities being inaccessible to subscribers.

Further issues identified related to outdated and unsupported software on the network. Both operating systems, along with installed software packages, were found to be out of date. An additional area of concern related to the use of outdated and in some cases, known vulnerable, communication protocols. Not only might these issues provide an alternative, or complementary, avenue of attack when seeking to compromise the network; they may also be used to impact the provision of the critical national infrastructure that NGPEW maintains.

It is strongly recommended that all software used within the enterprise is updated on a regular basis. System users should understand their own responsibilities regarding maintaining software and be reminded of this on a regular basis.

[redacted] offer the recommendation that it would be in the best interest of NGPEW and service users to remediate all issues highlighted within this report to enhance the overall security posture offered.

Finally, the findings in this report were obtained from a limited period of security testing as defined within the scope of work. A malicious attacker is unlikely to be constrained by either timescales or ethical considerations.

Risk Ratings

The table below has been generated to provide an insight into the risk rating and scoring system used throughout this report to help provide a concise and simple overview.

It should be noted that issues have been rated based on the evidence discovered by the testers and whilst there may be controls in place in the backend of the systems to prevent specific attacks occurring, these may not have been known to the tester throughout the assessment.

Risk Rating	**CVSSv3 Score**	**Description**
Critical	10.0 - 9.0	This requires resolution as quickly as possible
High	8.9 - 7.0	This requires resolution soon
Medium	6.9 - 4.0	This requires resolution in the medium term
Low	3.9 - 1.0	This requires resolution as part as routine maintenance
Informational	0.9 - 0	This requires resolution to be in line with best practices

Calculating Risk

The risk rating is calculated by measuring the impact and probability of an attack occurring:

Risk = Impact * Probability

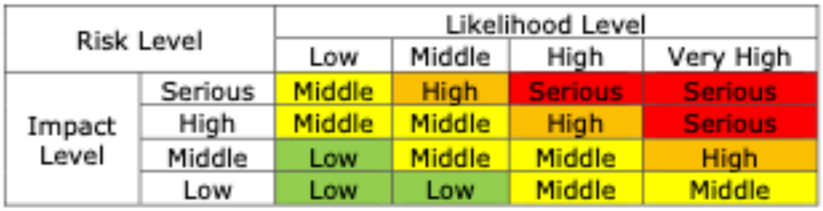
Impact

The impact is represented through qualitative methods, which range across four different levels (low, medium, high, and extreme)

Probability

The probability is the likelihood of a risk occurring, with qualitative probability ranging across five different levels (negligible, low, medium, high, and extreme).

To help calculate what the risk is against the system, the following matrix can be used:



Risk Level		Likelihood Level			
		Low	Middle	High	Very High
Impact Level	Serious	Middle	High	Serious	Serious
	High	Middle	Middle	High	Serious
	Middle	Low	Middle	Middle	High
	Low	Low	Low	Middle	Middle

Summary of Findings

The following tables summarise the issues identified throughout testing:

Critical	High	Medium	Low	Informational	Total
5	6	5	0	1	17

Issue	Severity	Recommendation
VNC server without authentication, as administrator	Critical	Implement authentication for VNC sessions
Unsupported version of Windows & IIS in use	Critical	Upgrade to a supported version of Windows & IIS
IIS password policy bypass present	Critical	Install updates
Endpoint security disabled	Critical	Enable the installed endpoint security program
Password reuse	Critical	Implement more stringent password guidelines
Outdated software in use	High	Update the software packages
Firewall ACLs overly permissive	High	Modify the ACLs to be more restrictive in segregation
Applications available over HTTP only	High	Configure the web servers to support only HTTPS
MODBUS accessible without any safeguards	High	Disable MODBUS in favour of a more secure alternative or segregate network
Java debugging server enabled	High	Disable the debugging interface
Insecure HTTP methods enabled	High	Disable unnecessary HTTP methods
ICS data accessible	Medium	Require user authentication
Excessive open ports	Medium	Whitelist open ports
Verbose Error Messages	Medium	Obfuscate error messages
Password policy & examples present on website	Medium	Remove the examples and policy
Reverse DNS enabled for all IP ranges	Medium	Remove unnecessary pointer records
Company documents discovered through OSINT	Informational	Completely delete the GitHub repository or remove the commits

Findings and Technical Details

The following section details vulnerabilities found throughout the testing phase, with the associated technical details. The following information is included, where applicable:

- **Risk Rating:** An overall rating of the risk posed to the customer by the issue
- **CVSS v3 Score:** A numeric value applied to the severity that the issue poses. [redacted] utilise the common vulnerability scoring system ("CVSS") version 3 by default
- **Description:** A high-level overview of the issue type
- **Details:** Specific details of the vulnerability as it applies to the customer's own environment, along with any steps that the customer can take to recreate the specific issue
- **Affected Hosts:** Information on the hosts or network services that were identified as being vulnerable
- **Issue Impact:** An indication of the impact that a customer might expect in the event of such an attack occurring
- **Recommendations:** Recommended actions to remediate the issue
- **References:** Additional references that may assist the customer in understanding the risks relating to the issue, and further information on how to remediate issues

VNC Server Available Without Authentication

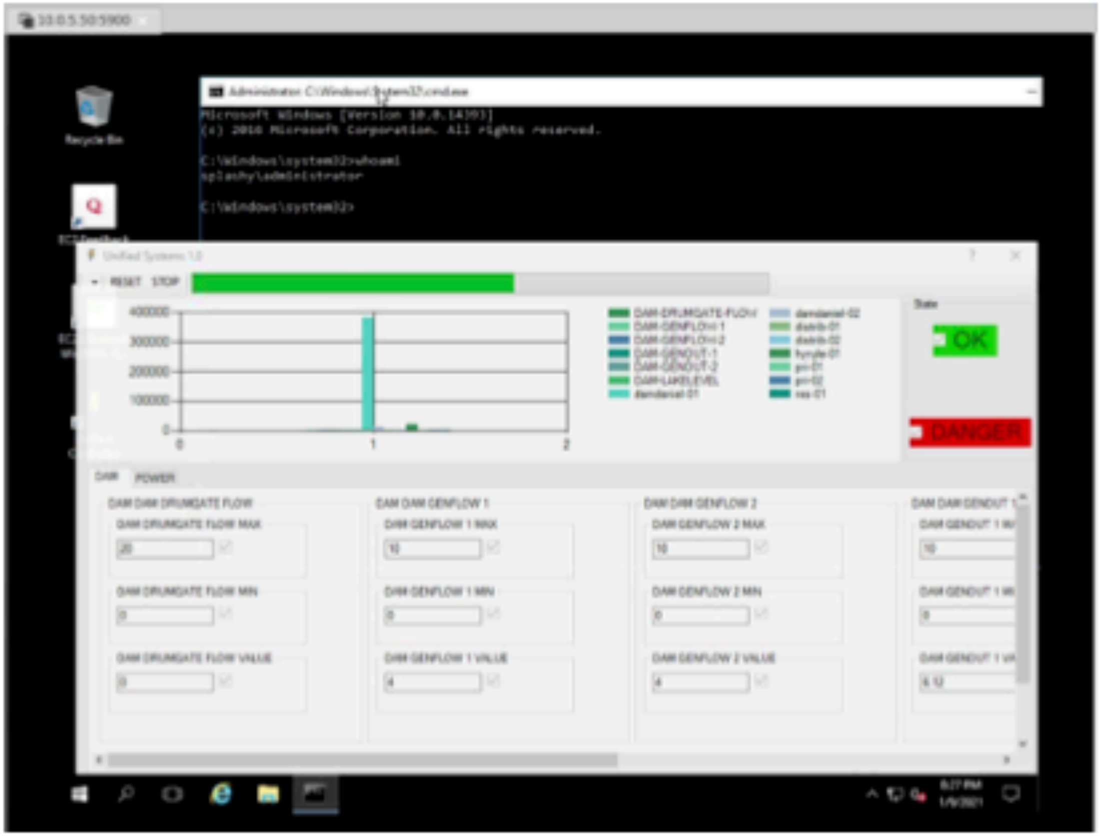
Risk Rating: **Critical** CVSS v3 Score: **10**

Issue Description:

The VNC server does not require authentication to connect to, allowing for unfettered access to the system by an unauthorised remote user. The user signed in on VNC is the local administrator, meaning that it is possible for an unauthorised user to obtain root level credentials. From there it's possible to obtain persistence within the network by adding a user account or retrieving the password hash of the inbuilt administrator account.

Details:

The installed VNC server allows an attacker to connect with no authentication, to a local administrator level account.



```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
splashy\administrator

C:\Windows\system32>
```

DAM DAM DRUMGATE FLOW
DAM DRUMGATE FLOW MAX: 20
DAM DRUMGATE FLOW MIN: 0
DAM DRUMGATE FLOW VALUE: 0

DAM DAM GENFLOW 1
DAM GENFLOW 1 MAX: 10
DAM GENFLOW 1 MIN: 0
DAM GENFLOW 1 VALUE: 4

DAM DAM GENFLOW 2
DAM GENFLOW 2 MAX: 10
DAM GENFLOW 2 MIN: 0
DAM GENFLOW 2 VALUE: 4

DAM DAM GENOUT 1
DAM GENOUT 1 M: 10
DAM GENOUT 1 M: 0
DAM GENOUT 1 VA: 6.12

Affected Hosts:

IP Address	Port
10.0.10.50	5900/TCP

Issue Impact:

This issue has potential to impact confidentiality, integrity, and availability, since there may be sensitive information stored on the PC, and it is possible to modify the information, which could also be done in such a way to disable the PC or devices connected to the PC.

The potential impacts of a successful attack of this nature are:

- System compromise
- Theft of confidential data
- Lack of service availability

Issue Reproduction:

To reproduce this issue, use a VNC client such as TightVNC to connect to port 5900 on the affected machine.

Recommendations:

It is strongly recommended to implement a form of authentication on the VNC. This will contribute to defence in depth so that even if an attacker gains access to the internal network, sensitive assets are still safeguarded, and they will not be able to escalate their privileges. If possible, the user available through VNC should not be an administrator and should have the minimum privilege level possible to complete the required tasks.

References:

VNC Null Authentication Access	https://www.fortiguard.com/encyclopedia/ips/31552/vnc-server-null-authentication-access
Vulnerability Note VU#117929	https://www.kb.cert.org/vuls/id/117929

Unsupported Versions of Windows and IIS in Use

Risk Rating: **Critical** CVSS v3 Score: **10**

Issue Description:

The host was identified as running an operating system and software that is no longer under active support by the vendor responsible. Unsupported software will no longer receive updates and subsequently, any security issues that are identified with the software will not receive patches to resolve those issues. Failure to maintain regular upstream updates vastly increases the risk of successful compromise by a malicious party.

Details:

The host indicated below was identified as running an operating system (Microsoft Windows NT 4.0) and software (IIS version 4.0) that is no longer under vendor support. As such, this host will no longer receive updates and is at risk of compromise should any vulnerabilities be identified.

```
CPE: cpe:/o:microsoft:windows-nt:4.0
```

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/4.0
PICS-Label: (PICS-1.0 "http://www.rsac.org/ratingsv01.html" l by
"easteregg@jrwr.io" on "2020.09.04T03:21--100" exp
"2021.09.04T12:00--100" r (v 0 s 0 n 0 l 4))
Cache-Control: max-age=1800:
```

Affected Hosts:

IP Address
10.0.10.152

Issue Impact:

This issue has the potential to impact upon the confidentiality, integrity, and availability of the host. Secondary impact to other business systems may also be possible in the event of a vulnerability allowing system compromise leading to lateral network movement.

The potential issues arising from a successful attack of this nature are:

- System compromise arising from remote code execution vulnerabilities
- Theft of confidential data from compromised systems
- Lack of service availability due to denial-of-service attacks

Issue Reproduction:

To verify this issue, use a network scanner such as nmap to fingerprint the operating system, and a network protocol tester such as curl to view the headers of a webpage served by the host.

Recommendations:

Replace the operating system and software with some that is still within the vendor support period. If business reasons dictate that the affected host must remain within the environment whilst the migration occurs, ensure that the host is suitably isolated, with strict access control rules in place to limit the attackable surface area presented by the host.

References:

Support for Windows NT Server 4.0	https://news.microsoft.com/2004/12/03/q-exchange-server-5-5-to-follow-in-one-year/
IIS 4.0 Vulnerabilities	https://www.cvedetails.com/vulnerability-list.php?vendor_id=26&product_id=63&version_id=694

IIS Password Policy Bypass Present

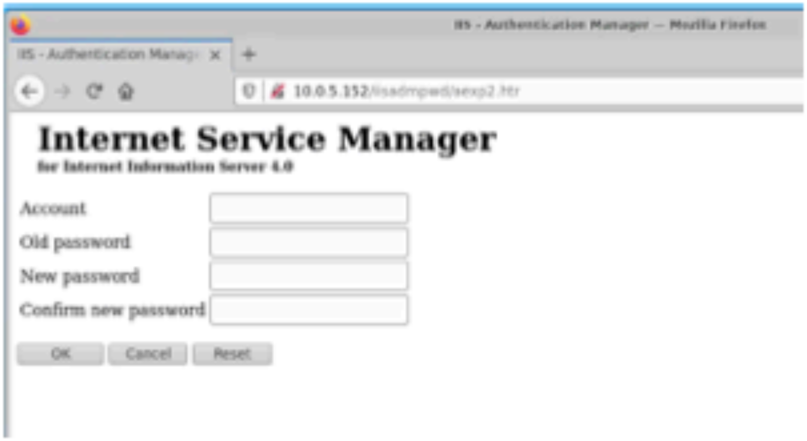
Risk Rating: **Critical** CVSS v3 Score: **9.5**

Issue Description:

By default, this version of IIS installs the password change file by default, which could be abused by an attacker to brute force a valid username or password, gaining unauthorised access. A legitimate user could also abuse this to set a password that may not be compliant with the password policy of the host or change the password on a locked account – successfully unlocking it and regaining access without the administrator having knowledge of this.

Details:

The password change file was accessible through IIS without any other user authentication.


IIS - Authentication Manager — Mozilla Firefox
IIS - Authentication Manag
10.0.5.152/iisadmpwd/aexp2.htr
Internet Service Manager
for Internet Information Server 4.0
Account
Old password
New password
Confirm new password
OK
Cancel
Reset

Affected Hosts:

IP Address
10.0.10.152

Issue Impact:

This issue has the potential to impact upon the confidentiality, and integrity of the host.

The potential issues arising from a successful attack of this nature are:

- Theft of confidential data from compromised systems
- Unauthorised modification of user account attributes

Issue Reproduction:

To reproduce this issue, browse to this page on the host, in a modern web browser such as Firefox:

Iisadmpwd/aexp2.htr

Recommendations:

Remove the HTR mapping from IIS to prevent the files from being served by IIS.

References:

Bugtraq thread	https://seclists.org/bugtraq/2002/Mar/113
CVE-1999-0407	https://nvd.nist.gov/vuln/detail/CVE-1999-0407

Endpoint Security Disabled

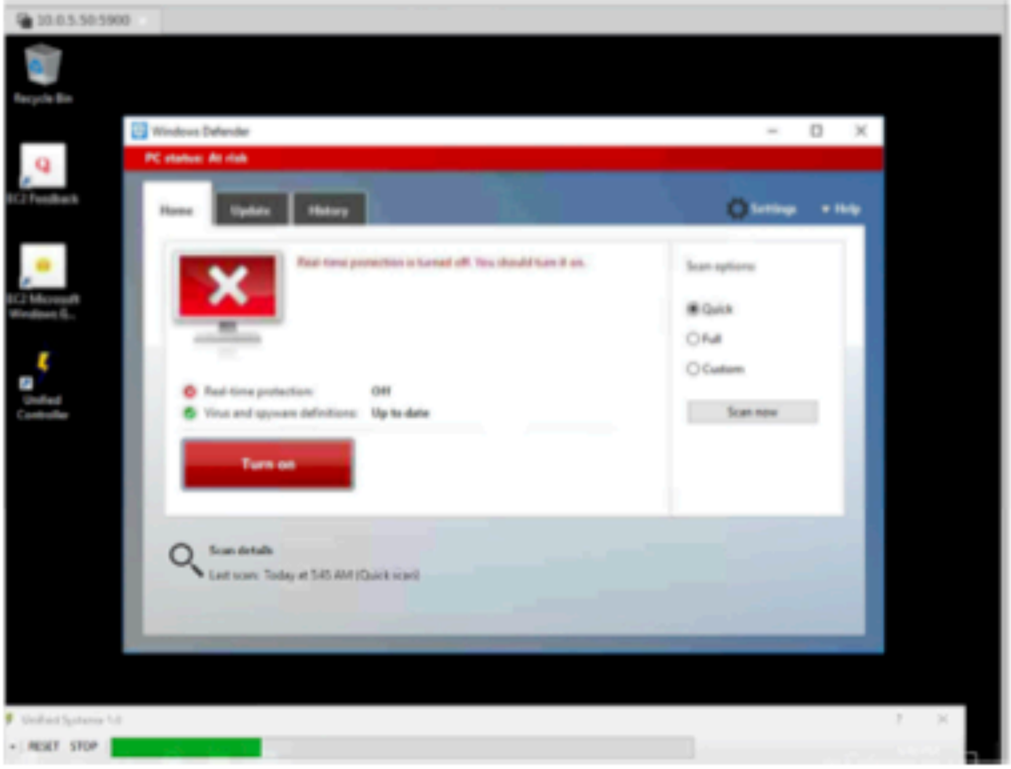
Risk Rating: **Critical** CVSS v3 Score: **9.3**

Issue Description:

The installed endpoint security solution on the host was found to be disabled. This means that the host does not have a functional anti-virus solution present, which means that common exploits may not be stopped, leading to compromise of the machine, and all files within.

Details:

Windows Defender real time protection was disabled on the host.



PC status: At risk

Real-time protection is turned off. You should turn it on.

Real-time protection: Off
Virus and spyware definitions: Up to date

Scan options:
● Quick
○ Full
○ Custom

Scan details
Last scan: Today at 5:45 AM (Quick scan)

Affected Hosts:

IP Address
10.0.1.10
10.0.1.11
10.0.1.13
10.0.5.50

Issue Impact:

This issue has the potential to impact upon the confidentiality, and integrity of the host through a successful malware attack – for example:

- Theft of confidential data from compromised systems
- Unauthorised modification of files from malware activity

Issue Reproduction:

To verify this issue, view the Windows Defender settings within Windows.

Recommendations:

Enable the real-time protection in Windows Defender or implement a third-party antivirus solution.

References:

Enabling real time protection	https://onlinehelp.opswat.com/metaaccess/Windows_Defender-real_time_protection_disabled.html
Importance of Antivirus	https://blog.reasonsecurity.com/2020/01/12/why-is-antivirus-software-important/

Password Reuse

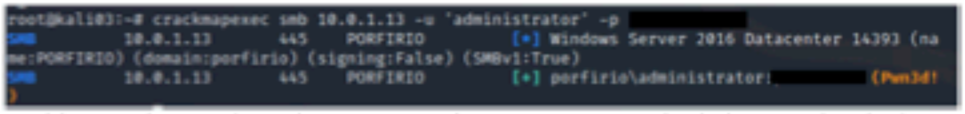
Risk Rating: **Critical** CVSS v3 Score: **9.1**

Issue Description:

Passwords were found to be reused across machines.

User passwords provide an important layer of protection against network-based attacks. It is important that users are required to maintain secure and unique passwords to prevent them from being guessed or intercepted by any attackers able to gain network access or lateral movement. Password policies should include such areas as password length, complexity, and appropriate aging, as well as stipulate that a unique password should be used in each instance.

Details:



```
root@kali03:~# crackmapexec smb 10.0.1.13 -u 'administrator' -p [redacted]
SMB         10.0.1.13       445    PORFIRIO         [*] Windows Server 2016 Datacenter 14393 (na
me:PORFIRIO) (domain:porfirio) (signing:False) (SMBv1:True)
SMB         10.0.1.13       445    PORFIRIO         [+] porfirio\administrator:[redacted] (Pwn3d!
)
```

It was possible to utilise credential spraying to obtain access to multiple hosts at local administrator privilege.

Affected Hosts:

IP Address
10.0.1.10
10.0.1.11
10.0.1.13
10.0.5.50

Issue Impact:

This issue has the potential to impact upon the confidentiality of user data.

The potential issues arising from a successful attack of this nature are:

- Loss of confidentiality in any resources secured by an account password
- Increased likelihood of an attacker gaining access to sensitive resources when masquerading as a legitimate user
- The theft or modification of sensitive data accessible by a compromised account
- A loss of integrity in any additional services that the compromised account has access to

Issue Reproduction:

To verify this issue, log into each machine with the local administrator account, using the same password.

Recommendations:

A suitably secure password policy should be created and enforced across the organisation. The policy should be communicated to all users for awareness, and users should also be trained in the reasons as to why selecting a secure password is important. Password guidance changes periodically as new techniques are discovered to attack user credentials, so further research on the most business-appropriate policies should always be undertaken. However, at the time of writing, the general advice provided by [redacted] suggests that passwords should:

- Be unique in each instance
- Be a minimum of 14 characters long
- Contain a mixture of upper- & lower-case characters, along with numbers and special characters. In an Active Directory environment, ensure that the password complexity requirements are enabled and deployed domain-wide using group policy
- Lock out their respective accounts after five unsuccessful login attempts. Accounts should lock out for a minimum of 15 minutes. The lockout timer should reset if further unsuccessful attempts are made during this time

References:

NCSC Password Guidance	https://www.ncsc.gov.uk/collection/passwords
A Study on Password Creation Behaviour	http://cups.cs.cmu.edu/rshay/pubs/Feedback.pdf

Outdated Software in Use

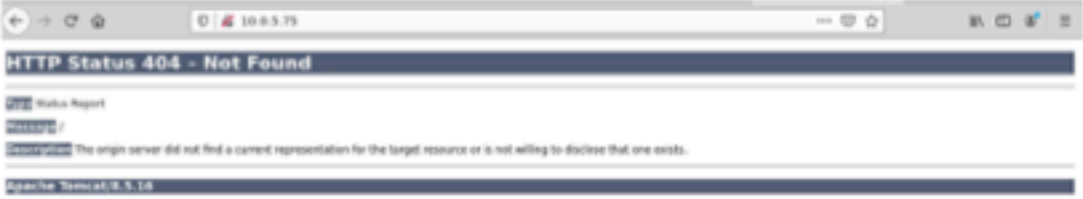
Risk Rating: **High** CVSS v3 Score: **8.3**

Issue Description:

Software installed within an enterprise requires regular and timely updates to reduce the risk of compromise from attack. A failure to incorporate third-party software into the patching cycle (patching only host operating systems) greatly increases the prospect of a successful attack. Vulnerabilities arising from outdated or vulnerable software may permit an attacker to deny the use of a platform to legitimate users, steal confidential data from a system, or potentially execute code against a system in order to compromise it in its entirety.

Details:

An outdated version of Apache web server was found to be in use, as well as an out of date version of MariaDB and Apache Tomcat.



10.0.5.75

HTTP Status 404 – Not Found

Type Status Report

Message /

Description The origin server did not find a current representation for the target resource or is not willing to disclose that one exists.

Apache Tomcat/8.5.16

Affected Hosts:

IP Address	Port
10.0.5.75	80/TCP, 3306/TCP
10.0.5.153	80/TCP

Issue Impact:

This issue has the potential to impact upon the confidentiality, integrity, and availability of the host. Secondary impact to other business systems may also be possible in the event of a vulnerability allowing system compromise leading to lateral network movement.

The potential issues arising from a successful attack of this nature are:

- System compromise arising from remote code execution vulnerabilities
- Theft of confidential data from compromised systems
- Lack of service availability because of denial-of-service attacks

Issue Reproduction:

To verify this issue, visit each website to view the current software versions, and use a network scanner such as nmap to view the banner of the affected MariaDB service.

Recommendations:

Third-party software products should be audited regularly and incorporated into an organisation's patching cycle. An effective patching cycle should be underpinned by the appropriate policy and communicated to all members of staff for awareness.

References:

Apache	https://www.apachelounge.com/Changelog-2.4.html
MariaDB	https://downloads.mariadb.org/mariadb/+releases/
Tomcat	https://tomcat.apache.org/tomcat-8.5-doc/changelog.html

Firewall ACLs Overly Permissive

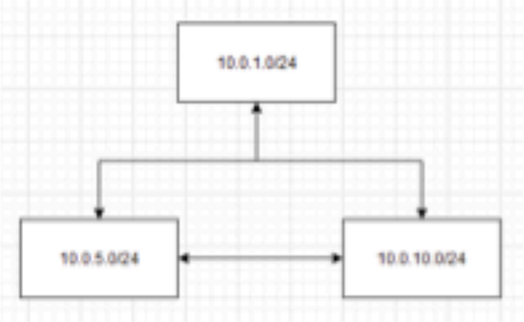
Risk Rating: **High** CVSS v3 Score: **8.3**

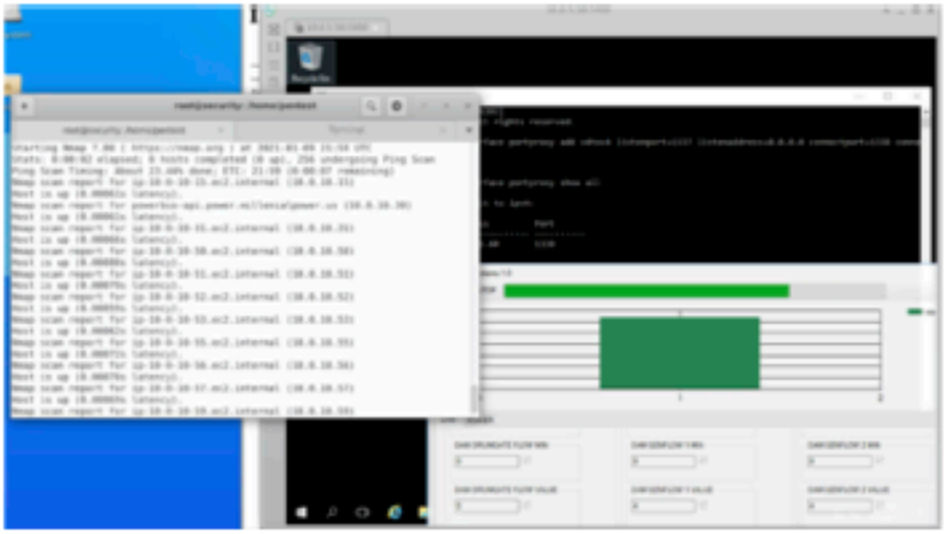
Issue Description:

The firewall policies in place were found to be overly permissive in places, allowing more access than the bare minimum required to perform required operations. A malicious party could potentially be granted more access to internal networks due to the broader scope of the firewall policies – leading to an increased attack surface and therefore risk to the organisation.

Details:

It was possible to access both the 10.0.5.0/24 and 10.0.10.0/24 subnets from machines on the 10.0.1.0/24 subnet. The below diagram represents this in more detail. No protocol restrictions were encountered, and all ports were accessible from each subnet to the others.





```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-09 15:54 UTC
Stats: 0:00:02 elapsed; 8 hosts completed (8 up), 256 undergoing Ping Scan
Ping Scan Timing: About 23.40% done; ETC: 21:59 (0:00:07 remaining)
Nmap scan report for ip-10-0-10-15.ec2.internal (10.0.10.15)
Host is up ([illegible] latency).
Nmap scan report for powerbus-api.power.millenialpower.us (10.0.10.30)
Host is up ([illegible] latency).
Nmap scan report for ip-10-0-10-31.ec2.internal (10.0.10.31)
Host is up ([illegible] latency).
Nmap scan report for ip-10-0-10-50.ec2.internal (10.0.10.50)
Host is up ([illegible] latency).
Nmap scan report for ip-10-0-10-51.ec2.internal (10.0.10.51)
Host is up ([illegible] latency).
Nmap scan report for ip-10-0-10-52.ec2.internal (10.0.10.52)
Host is up ([illegible] latency).
Nmap scan report for ip-10-0-10-53.ec2.internal (10.0.10.53)
Host is up ([illegible] latency).
Nmap scan report for ip-10-0-10-55.ec2.internal (10.0.10.55)
Host is up ([illegible] latency).
Nmap scan report for ip-10-0-10-56.ec2.internal (10.0.10.56)
Host is up ([illegible] latency).
Nmap scan report for ip-10-0-10-57.ec2.internal (10.0.10.57)
Host is up ([illegible] latency).
Nmap scan report for ip-10-0-10-59.ec2.internal (10.0.10.59)
```

Affected Hosts:

IP Address
10.0.1.0/24
10.0.5.0/24
10.0.10.0/24

Issue Impact:

This issue has the potential to impact upon the confidentiality of the network. Secondary impact to other business systems may also be possible through lateral movement by an attacker leading to further exploitation of machines on the network.

The potential issues arising from a successful attack of this nature are:

- Theft of confidential data from compromised systems
- Lack of service availability because of denial-of-service attacks

Issue Reproduction:

To verify this issue, ping a machine on each subnet from a machine on another subnet.

Recommendations:

The default rule for the firewall should be deny, with as granular access control rules as possible for exceptions – only when there is a clear and documented business need. Regular firewall reviews should be performed, to avoid legacy rules being left on the firewall, increasing the attack surface.

References:

Firewall rule best practices	https://www.liquidweb.com/kb/best-practices-for-firewall-rules/

Applications Available Over HTTP Only

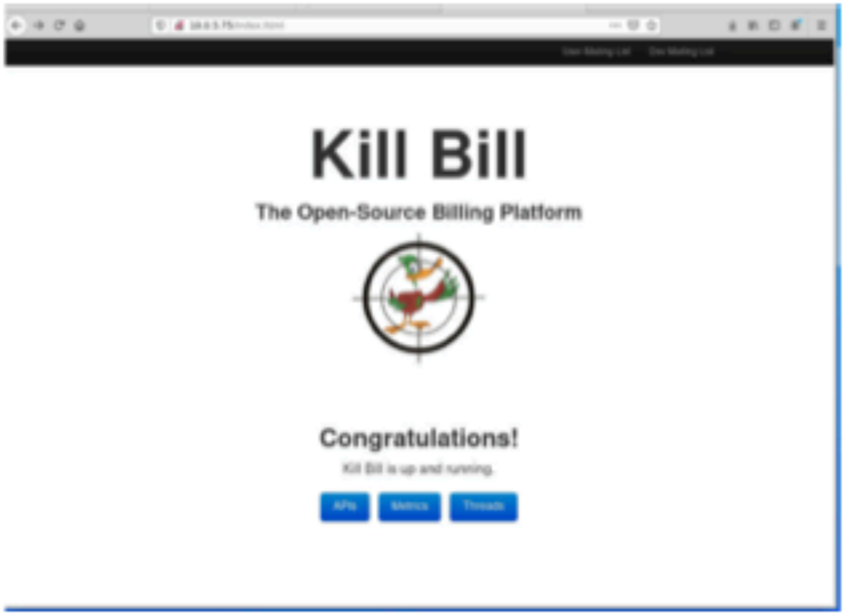
Risk Rating: **High** CVSS v3 Score: **8.2**

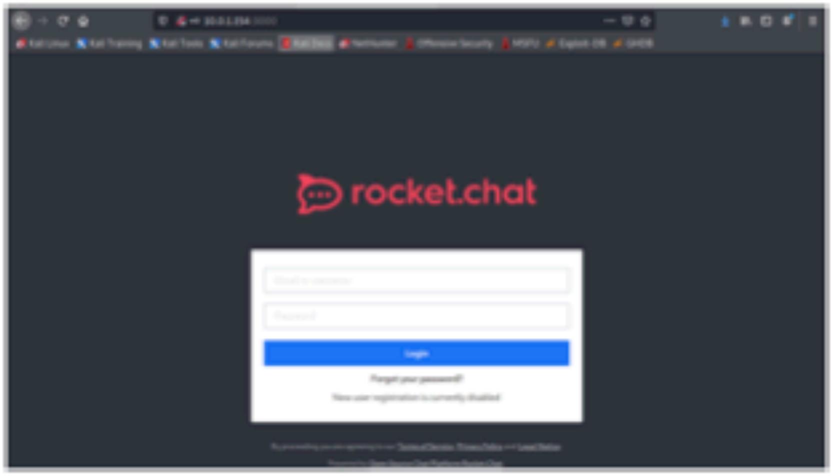
Issue Description:

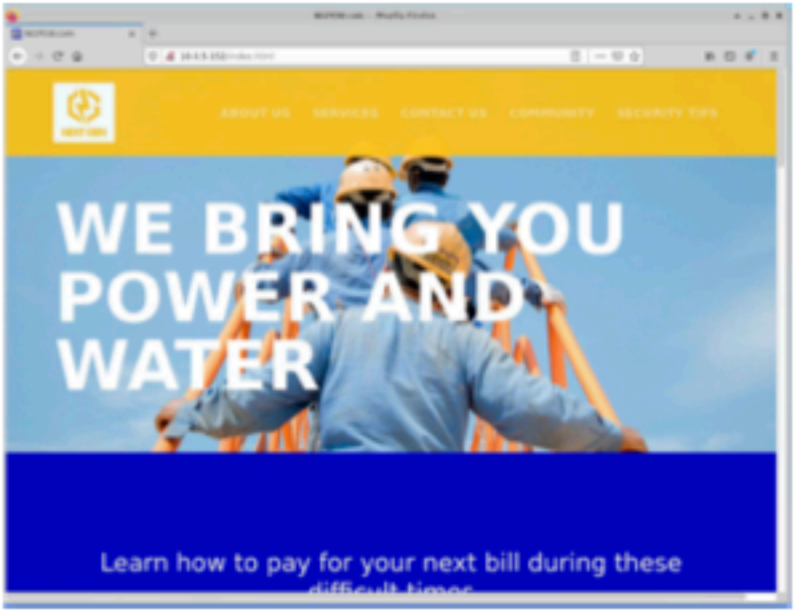
Applications serve content over an insecure network protocols. The web application should always be protected with HTTPS, even if they do not handle sensitive communications. Aside from providing critical security and data integrity for both your websites and your users' personal information, HTTPS is a requirement for many new browser features, particularly those required for progressive web apps.

Details:

It was only possible to access RocketChat, Kill Bill and the NGPEW website through HTTP.







Learn how to pay for your next bill during these difficult times

Affected Hosts:

IP Address	Port
10.0.1.154	3000/TCP
10.0.5.75	80/TCP, 8080/TCP
10.0.5.152	80/TCP

Issue Impact:

This issue has the potential to impact upon the confidentiality of the web application, because data is transferred between the server and the client in clear text. There is secondary impact to the web integrity if credentials can be intercepted.

The potential issues arising from a successful attack of this nature are:

- Application compromise through the interception of administrative user credentials
- Data loss, destruction, or exfiltration
- Financial impact with regards to the support costs anticipated in dealing with the clean up after such an attack
- Reputational damage arising from reduced customer confidence in the aftermath of a successful attack

Issue Reproduction:

To reproduce this issue, browse to the hosts in a modern web browser such as Firefox**.**

Recommendations:

HTTPS should be utilised. An SSL certificate should be purchased and installed on the affected web services, and secure TLS settings should be used on the web servers to avoid the possibility of a LOGJAM attack or similar.

References:

Firewall rule best practices	https://www.liquidweb.com/kb/best-practices-for-firewall-rules/

MODBUS Accessible

Risk Rating: **High** CVSS v3 Score: **8.1**

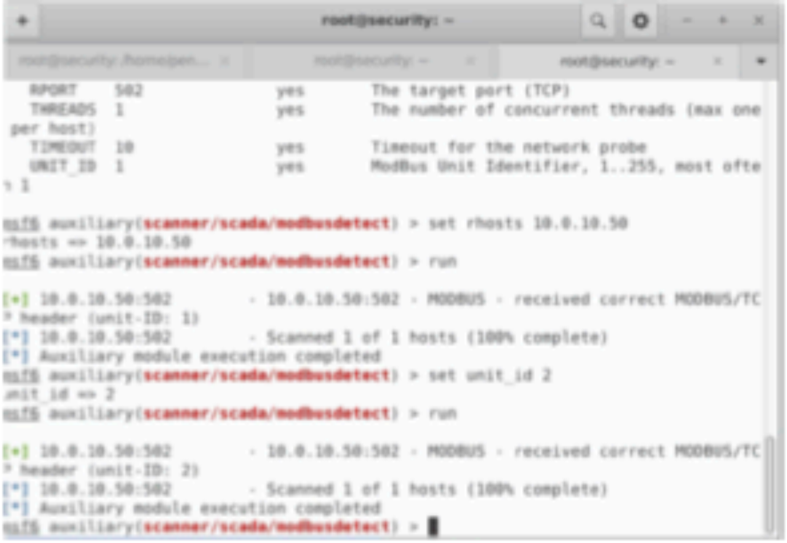
Issue Description:

MODBUS is an old protocol with no inbuilt authentication or encryption, making it trivial for an attacker to intercept or modify.

Details:

Devices using MODBUS over TCP were identified by the testing team. It was possible to run queries against the devices, proving that there was connectivity to them across the network.

It's important to note that the devices on the network seemed to be using a custom implementation of MODBUS, so verification was only possible through tooling.

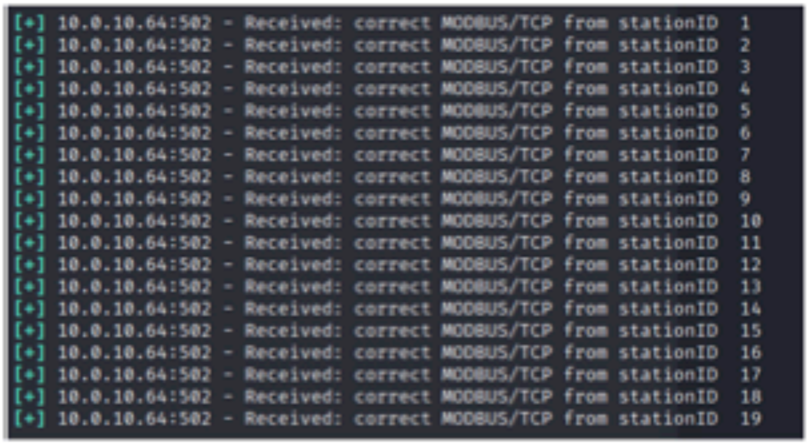


```
   RPORT    502              yes       The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (max one
 per host)
   TIMEOUT  10               yes       Timeout for the network probe
   UNIT_ID  1                yes       ModBus Unit Identifier, 1..255, most ofte
n 1

msf6 auxiliary(scanner/scada/modbusdetect) > set rhosts 10.0.10.50
rhosts => 10.0.10.50
msf6 auxiliary(scanner/scada/modbusdetect) > run

[+] 10.0.10.50:502        - 10.0.10.50:502 - MODBUS - received correct MODBUS/TC
P header (unit-ID: 1)
[*] 10.0.10.50:502        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/scada/modbusdetect) > set unit_id 2
unit_id => 2
msf6 auxiliary(scanner/scada/modbusdetect) > run

[+] 10.0.10.50:502        - 10.0.10.50:502 - MODBUS - received correct MODBUS/TC
P header (unit-ID: 2)
[*] 10.0.10.50:502        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/scada/modbusdetect) > 
```



```
[+] 10.0.10.64:502 - Received: correct MODBUS/TCP from stationID  1
[+] 10.0.10.64:502 - Received: correct MODBUS/TCP from stationID  2
[+] 10.0.10.64:502 - Received: correct MODBUS/TCP from stationID  3
[+] 10.0.10.64:502 - Received: correct MODBUS/TCP from stationID  4
[+] 10.0.10.64:502 - Received: correct MODBUS/TCP from stationID  5
[+] 10.0.10.64:502 - Received: correct MODBUS/TCP from stationID  6
[+] 10.0.10.64:502 - Received: correct MODBUS/TCP from stationID  7
[+] 10.0.10.64:502 - Received: correct MODBUS/TCP from stationID  8
[+] 10.0.10.64:502 - Received: correct MODBUS/TCP from stationID  9
[+] 10.0.10.64:502 - Received: correct MODBUS/TCP from stationID  10
[+] 10.0.10.64:502 - Received: correct MODBUS/TCP from stationID  11
[+] 10.0.10.64:502 - Received: correct MODBUS/TCP from stationID  12
[+] 10.0.10.64:502 - Received: correct MODBUS/TCP from stationID  13
[+] 10.0.10.64:502 - Received: correct MODBUS/TCP from stationID  14
[+] 10.0.10.64:502 - Received: correct MODBUS/TCP from stationID  15
[+] 10.0.10.64:502 - Received: correct MODBUS/TCP from stationID  16
[+] 10.0.10.64:502 - Received: correct MODBUS/TCP from stationID  17
[+] 10.0.10.64:502 - Received: correct MODBUS/TCP from stationID  18
[+] 10.0.10.64:502 - Received: correct MODBUS/TCP from stationID  19
```

Affected Hosts:

IP Address	Port
10.0.10.50-65	502/TCP

Issue Impact:

This issue has the potential to impact upon the integrity of the ICS systems through unauthorised modifications.

The potential issues arising from a successful attack of this nature are:

- Lack of service availability
- Financial impact with regards to the support costs anticipated in dealing with the clean up after such an attack
- Reputational damage arising from reduced customer confidence in the aftermath of a successful attack

Issue Reproduction:

To reproduce this issue, utilise a MODBUS scanner such as the script in nmap or the auxiliary module in Metasploit (scanner/scada/modbus_findunitid).

Recommendations:

MODBUS should be disabled in favour of its more modern and secure updated version. If this is not possible, devices communicating using it should be segregated from the main network, with a strong ACL in place to reduce the attack surface.

References:

MODBUS Security	https://blog.se.com/machine-and-process-management/2018/08/30/modbus-security-new-protocol-to-improve-control-system-security/
Evolving towards secure MODBUS	https://www.incibe-cert.es/en/blog/evolving-towards-secure-modbus

Java Debugging Server Accessible

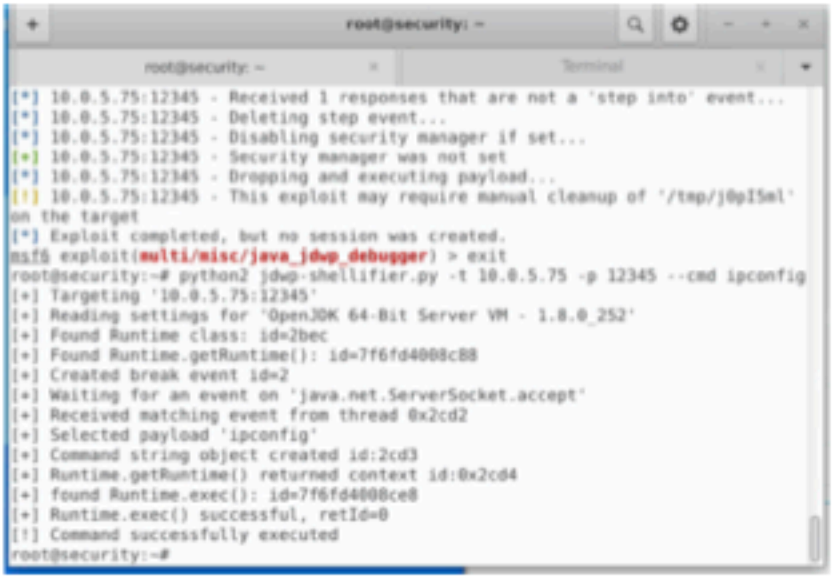
Risk Rating: **High** CVSS v3 Score: **7.2**

Issue Description:

The Java Debug Wire Protocol (JDWP) is a communication protocol that exists to connect the Java VM Tool Interface to a debugger console. It allows low level access to the host running the Java server, and has no built-in authentication or logging, which makes it relatively simple for an attacker to exploit.

Details:

It was possible to connect to the JDWP interface on the host, and obtain information about the server. Unfortunately due to tooling constraints, the pentest team was unable to exploit the service further and obtain full remote code execution, but it should be possible for a dedicated adversary to achieve this.



```
[*] 10.0.5.75:12345 - Received 1 responses that are not a 'step into' event...
[*] 10.0.5.75:12345 - Deleting step event...
[*] 10.0.5.75:12345 - Disabling security manager if set...
[+] 10.0.5.75:12345 - Security manager was not set
[*] 10.0.5.75:12345 - Dropping and executing payload...
[!] 10.0.5.75:12345 - This exploit may require manual cleanup of '/tmp/j0pI5ml'
on the target
[*] Exploit completed, but no session was created.
msf6 exploit(multi/misc/java_jdwp_debugger) > exit
root@security:~# python2 jdwp-shellifier.py -t 10.0.5.75 -p 12345 --cmd ipconfig
[+] Targeting '10.0.5.75:12345'
[+] Reading settings for 'OpenJDK 64-Bit Server VM - 1.8.0_252'
[+] Found Runtime class: id=2bec
[+] Found Runtime.getRuntime(): id=7f6fd4008c88
[+] Created break event id=2
[+] Waiting for an event on 'java.net.ServerSocket.accept'
[+] Received matching event from thread 0x2cd2
[+] Selected payload 'ipconfig'
[+] Command string object created id:2cd3
[+] Runtime.getRuntime() returned context id:0x2cd4
[+] found Runtime.exec(): id=7f6fd4008ce8
[+] Runtime.exec() successful, retId=0
[!] Command successfully executed
root@security:~#
```

Affected Hosts:

IP Address	Port
10.0.5.75	12345/TCP

Issue Impact:

This issue has the potential to impact upon the integrity of the host, as well as the confidentiality.

The potential issues arising from a successful attack of this nature are:

- Lack of service availability
- Application compromise through remote code execution
- Data loss, destruction, or exfiltration

Issue Reproduction:

To reproduce this issue, utilise this exploitation script in Python 2:
https://github.com/IOActive/jdwp-shellifier

Recommendations:

The JDWP debug server should be disabled.

References:

Hacking the Java Debug Wire Protocol	https://ioactive.com/hacking-java-debug-wire-protocol-or-how/

Insecure HTTP Methods Enabled

Risk Rating: **High** CVSS v3 Score: **7.1**

Issue Description:

Insecure HTTP methods other than GET and POST are enabled on the web server. These methods allow for additional functionality that could be used to conduct further attacks.

Details:

The web server has the PUT, DELETE, & TRACE methods enabled.

```
80/tcp   open   http
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD PUT DELETE POST
|_  Potentially risky methods: TRACE PUT DELETE
```

Affected Hosts:

IP Address	Port
10.0.5.152	80/TCP

Issue Impact:

This issue has the potential to impact upon the confidentiality of the system through unauthorised access.

The potential issues arising from a successful attack of this nature are:

- Data loss, destruction, or exfiltration
- Lack of service availability
- Financial impact with regards to the support costs anticipated in dealing with the clean up after such an attack

Issue Reproduction:

To reproduce this issue, use a network enumeration tool such as nmap to query the available HTTP methods (e.g. the http-methods script).

Recommendations:

The extra methods should be disabled.

References:

Unsafe HTTP Methods	https://www.onwebsecurity.com/security/unsafe-http-methods.html

ICS Data Accessible

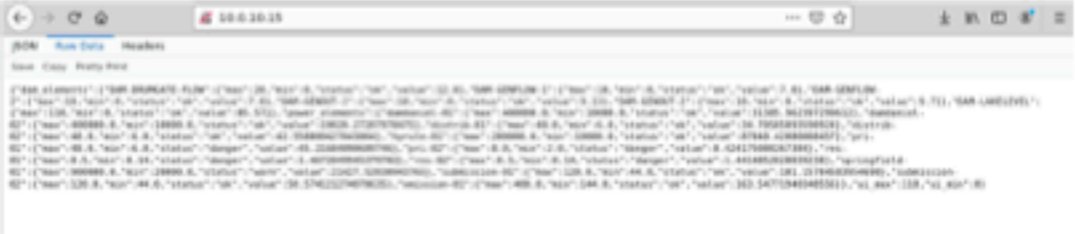
Risk Rating: **Medium** CVSS v3 Score: **6.5**

Issue Description:

It was possible to view statistics and other information about the microgrid controller. It may also be possible to modify parameters, though to avoid potential disruption to services, the pentest team did not attempt to validate this.

Details:

Browsing to the URL below within the application displays a JSON file of information about the ICS.



[illegible]

Affected Hosts:

IP Address	Port
10.0.10.15	80/TCP

Issue Impact:

This issue reflects an information leakage and does not adversely affect the security of the tested resources. It has been reported as an issue as it represents a lack of adherence to current best practice, as validation of modification has not been completed. Remediation of this issue will serve to further increase the security of the customer's environment.

The potential issues arising from a successful attack of this nature are:

- Technical information leakage, potentially assisting a malicious actor in targeting further attacks.

Issue Reproduction:

To reproduce this issue, visit the affected host in a modern web browser such as Firefox.

Recommendations:

Authentication should be used when accessing sensitive information – such as HTTP basic auth or bearer tokens.

References:

OWASP User Authentication Cheat Sheet	https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

Excessive Open Ports

Risk Rating: **Medium** CVSS v3 Score: **5.3**

Issue Description:

Excessive open ports can reflect a larger attack surface, and more potential vulnerabilities.

Details:

An example output can be found below:

```
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds  Microsoft Windows Server 2008 R2 - 2012
microsoft-ds
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
5900/tcp  open  vnc           VNC (protocol 3.8))
```

Affected Hosts:

IP Address
10.0.1.10
10.0.1.11
10.0.1.12
10.0.1.13
10.0.1.100
10.0.5.50
10.0.5.75
10.0.5.152

Issue Impact:

This issue reflects a minor information leakage and does not adversely affect the security of the tested resources. It has been reported as an issue as it represents a lack of adherence to current best practice. Remediation of this issue will serve to further increase the security of the customer's environment.

The potential issues arising from a successful attack of this nature are:

- Technical information leakage, potentially assisting a malicious actor in targeting further attacks.

Issue Reproduction:

To verify this issue, use a network enumeration tool such as nmap to scan the ports of the hosts.

Recommendations:

Ports should be whitelisted, with only necessary ones opened to the network.

References:

Open Port Vulnerabilities	https://www.bitsight.com/blog/open-port-vulnerabilities-whats-the-big-deal

Verbose Error Messages

Risk Rating: **Medium** CVSS v3 Score: **5.3**

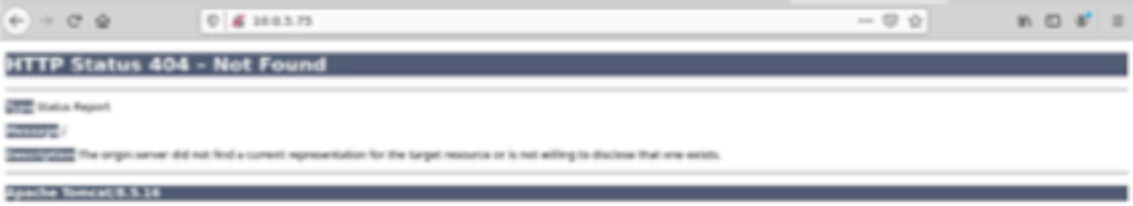
Issue Description:

Verbose error messages can provide an attacker useful information about the underlying infrastructure of the application and may include information such as: software versions, webroot paths, user context of the application and more.

Information such as this can lead to further targeted attacks against the application and greatly increase the targeted attack surface.

Details:

Browsing to the URL below within the application triggers an error which discloses the application is using Tomcat version 8.5.16.



HTTP Status 404 – Not Found

Type Status Report

Message /

Description The origin server did not find a current representation for the target resource or is not willing to disclose that one exists.

Apache Tomcat/8.5.16

Affected Hosts:

IP Address	Port
10.0.5.75	80/TCP
10.0.5.153	80/TCP

Issue Impact:

This issue reflects a minor information leakage and does not adversely affect the security of the tested resources. It has been reported as an issue as it represents a lack of adherence to current best practice. Remediation of this issue will serve to further increase the security of the customer's environment.

The potential issues arising from a successful attack of this nature are:

- Technical information leakage, potentially assisting a malicious actor in targeting further attacks.

Issue Reproduction:

To reproduce this issue, visit the affected hosts in a modern web browser such as Firefox.

Recommendations:

All errors within the application should be handled gracefully and provide minimal information to the end-users. All sensitive information should be stored on internal log files to troubleshoot and diagnose the issue and should not be relayed to end-users of the application where applicable.

References:

Error Handling	https://www.owasp.org/index.php/Error_Handling
Error Handling Cheat Sheet	https://cheatsheetseries.owasp.org/cheatsheets/Error_Handling_Cheat_Sheet.html

Password Policy and Examples Present on Website

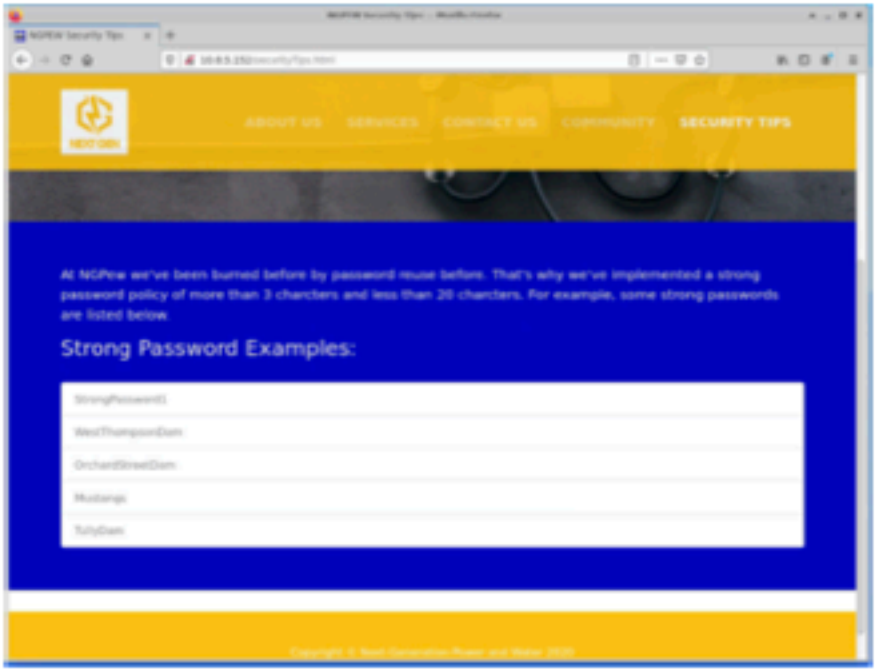
Risk Rating: **Medium** CVSS v3 Score: **5.3**

Issue Description:

Information about the password policy at NGPEW and examples of compliant passwords can be found on the website, which is publicly accessible, and available on the internal network. This information could be used by adversaries to tailor brute-force attacks to the password policy, increasing the chances of a successful attack.

Details:

The webpage can be found below:



At NGPew we've been burned before by password reuse before. That's why we've implemented a strong password policy of more than 3 charcters and less than 20 charcters. For example, some strong passwords are listed below.

Strong Password Examples:

StrongPassword1
WestThompsonDam
OrchardStreetDam
Mustangs
TullyDam

Copyright © Next Generation Power and Water 2020

Affected Hosts:

IP Address
10.0.5.152

Issue Impact:

This issue reflects a minor information leakage and does not adversely affect the security of the tested resources. It has been reported as an issue as it represents a lack of adherence to current best practice. Remediation of this issue will serve to further increase the security of the customer's environment.

The potential issues arising from a successful attack of this nature are:

- Technical information leakage, assisting a malicious actor in targeting further attacks.

Issue Reproduction:

To reproduce this issue, visit the affected hosts in a modern web browser such as Firefox.

Recommendations:

The page of the website should either be removed or have the information about the password policy removed.

References:

Information Disclosure	https://portswigger.net/web-security/information-disclosure

Reverse DNS Enabled for all IP Ranges

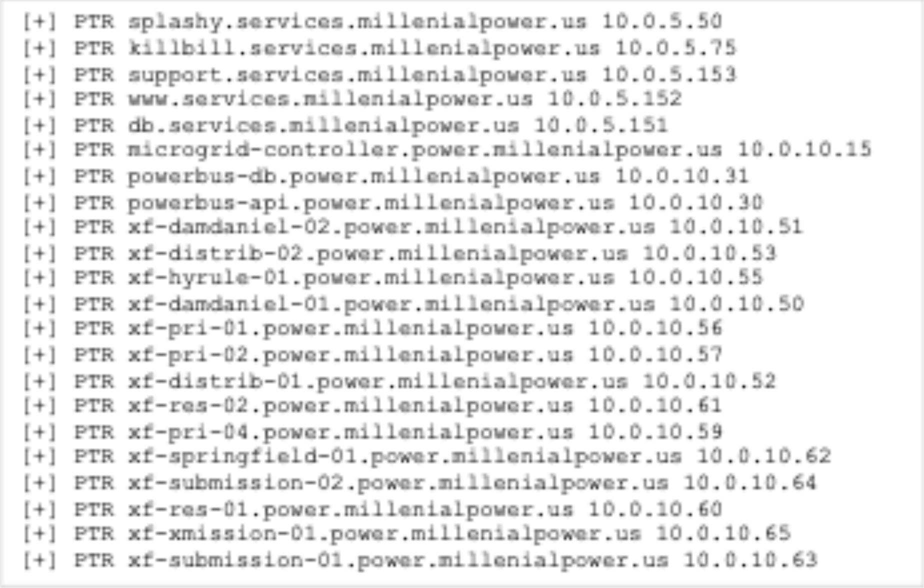
Risk Rating: **Medium** CVSS v3 Score: **4.3**

Issue Description:

Information about the purposes of hosts within the NGPEW network can be inferred by performing reverse DNS lookups. This information could be used by adversaries to tailor attacks to the hosts and the types of software that would be expected to be running on the systems, increasing the chances of a successful attack.

Details:

Output from bulk reverse lookups can be found below:



```
[+] PTR splashy.services.millenialpower.us 10.0.5.50
[+] PTR killbill.services.millenialpower.us 10.0.5.75
[+] PTR support.services.millenialpower.us 10.0.5.153
[+] PTR www.services.millenialpower.us 10.0.5.152
[+] PTR db.services.millenialpower.us 10.0.5.151
[+] PTR microgrid-controller.power.millenialpower.us 10.0.10.15
[+] PTR powerbus-db.power.millenialpower.us 10.0.10.31
[+] PTR powerbus-api.power.millenialpower.us 10.0.10.30
[+] PTR xf-damdaniel-02.power.millenialpower.us 10.0.10.51
[+] PTR xf-distrib-02.power.millenialpower.us 10.0.10.53
[+] PTR xf-hyrule-01.power.millenialpower.us 10.0.10.55
[+] PTR xf-damdaniel-01.power.millenialpower.us 10.0.10.50
[+] PTR xf-pri-01.power.millenialpower.us 10.0.10.56
[+] PTR xf-pri-02.power.millenialpower.us 10.0.10.57
[+] PTR xf-distrib-01.power.millenialpower.us 10.0.10.52
[+] PTR xf-res-02.power.millenialpower.us 10.0.10.61
[+] PTR xf-pri-04.power.millenialpower.us 10.0.10.59
[+] PTR xf-springfield-01.power.millenialpower.us 10.0.10.62
[+] PTR xf-submission-02.power.millenialpower.us 10.0.10.64
[+] PTR xf-res-01.power.millenialpower.us 10.0.10.60
[+] PTR xf-xmission-01.power.millenialpower.us 10.0.10.65
[+] PTR xf-submission-01.power.millenialpower.us 10.0.10.63
```

Affected Hosts:

IP Address
10.0.1.100 (DNS server queried)
10.0.5.0/24
10.0.10.0/24

Issue Impact:

This issue reflects a minor information leakage and does not adversely affect the security of the tested resources. It has been reported as an issue as it represents a lack of adherence to current best practice. Remediation of this issue will serve to further increase the security of the customer's environment.

The potential issues arising from a successful attack of this nature are:

- Technical information leakage, assisting a malicious actor in targeting further attacks.

Issue Reproduction:

To reproduce this issue, perform a reverse DNS lookup on an IP in an affected range.

Recommendations:

Unnecessary pointer records should be removed to reduce the risk profile.

References:

Reverse DNS	https://www.ionos.co.uk/digitalguide/server/know-how/reverse-dns/

Company Documents Discovered Through OSINT

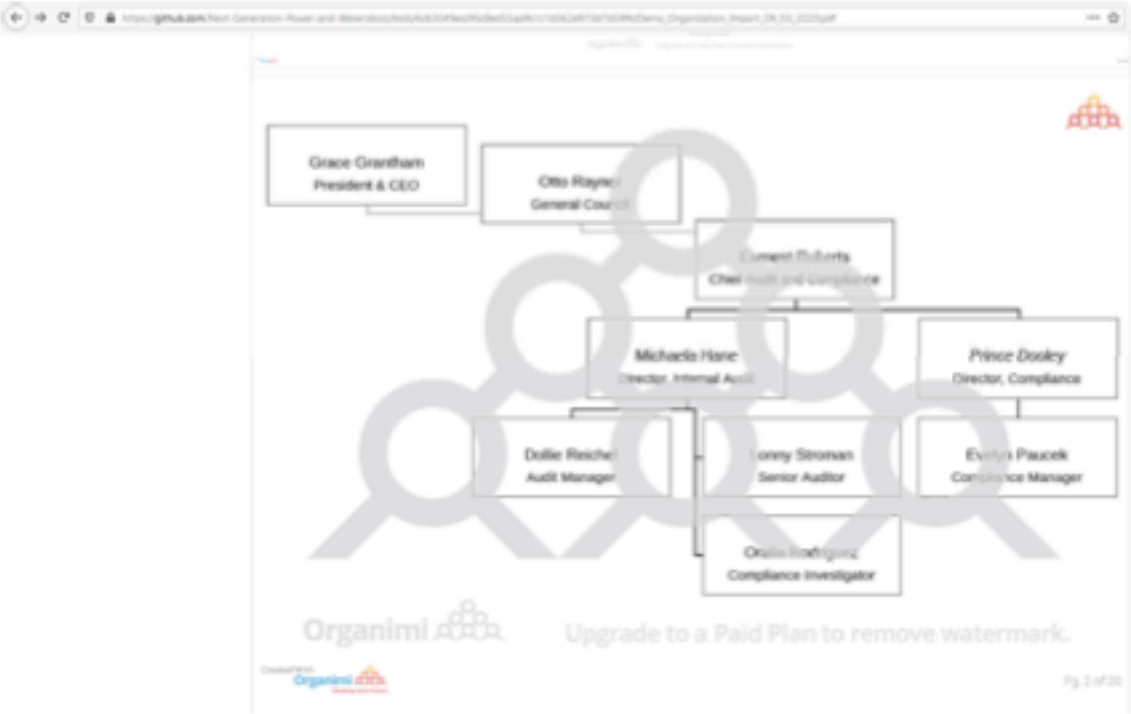
Risk Rating: **Informational** CVSS v3 Score: **0.0**

Issue Description:

It was possible to retrieve information about the organisation and the hierarchy of employees within through open-source intelligence efforts. It appears that an attempt was made to delete the files from the GitHub repository they were found in, but due to the nature of version control, a copy of the file is still saved within the repository.

Details:

An example page of the document can be seen below:



Affected Hosts:

URL
https://github.com/Next-Generation-Power-and-Water/docs
https://github.com/Next-Generation-Power-and-Water/docs/blob/6cb3049ecc95c8ed55aa9b1c1d362e975b7d59f4/Demo_Organization_Import_09_03_2020.pdf

Issue Impact:

This issue reflects a minor information leakage and does not adversely affect the security of the tested resources. It has been reported as an issue as it represents a lack of adherence to current best practice. Remediation of this issue will serve to further increase the security of the customer's environment.

The potential issues arising from a successful attack of this nature are:

- Technical information leakage, assisting a malicious actor in targeting further attacks.

Issue Reproduction:

To verify this issue, visit the GitHub repository as listed above in a modern web browser, such as Firefox.

Recommendations:

The GitHub repository should either be removed completely or have the commits containing the sensitive information deleted. Policies should be developed around the safe use of version control to avoid similar incidents occurring in future.

References:

Deleted files in Git	http://blog.kablamo.org/2013/12/08/git-restore/

Appendix

Appendix A: Infrastructure Testing Methodology

Fundamentals

An infrastructure assessment assesses for the vulnerabilities and weaknesses in the network configuration which are typically leveraged by malicious actors to gain full compromise of the internal domain. It provides an insight into an organisation's security posture.

An infrastructure assessment can be divided into three stages:

- Discovery
- Assessment
- Exploitation

Test Areas

[redacted]utilise a wide range of tools to scan and discover assets. Our testers use the latest scanning tools and techniques to perform a comprehensive audit of all IP ranges. Some of these include:

- TCP and UDP port scanning
- Operating system & service fingerprinting
- Network mapping
- User enumeration (where possible)

Once the discovery phase has ended, testers interpret the results and use them to identify possible attack vectors and perform manual attack simulations. Manual assessments focus on:

- Misconfigured hosts and services
- Patch level assessments
- Outdated systems and software
- Insecure protocols
- Weak passwords and default usernames
- LLMNR and NBNS spoofing

If a successful avenue of attack is identified, [redacted] will work with you to conduct safe exploitation (where possible) and verification of the issue whilst ensuring there are no disruptions to the daily running of your organisation. All exploitation is conducted under the agreed rules of the engagement.

Should a service be successfully exploited, [redacted]will aim to escalate to the highest of privileges and, with your agreement, continue to leverage this access to penetrate as deep as possible in your network to help portray a realistic attack scenario.

Appendix B: Tools Used

Tool Name	Version	Description
Nmap	7.91	Open source port scanning tool https://nmap.org/download.html
OpenVAS	20.8.0	Open source vulnerability scanner https://www.openvas.org/
Gobuster	3.1.0	Directory brute-force tool https://github.com/OJ/gobuster
Metasploit	4.19.0	Exploitation framework https://github.com/rapid7/metasploit-framework
Responder	2.0.7	LLMNR request poisoner https://github.com/lgandx/Responder
CrackMapExec	5.1.0	Enumeration and post exploitation framework https://github.com/byt3bl33d3r/CrackMapExec
Enum4Linux-ng	cc27bdb	Windows enumeration tool https://github.com/cddmp/enum4linux-ng
Crowbar	4.2	Brute-force tool https://github.com/galkan/crowbar
ProxyChains	4.3.0	Network pivoting tool https://github.com/haad/proxychains
Dnsrecon	0.9.1	DNS enumeration tool https://github.com/darkoperator/dnsrecon