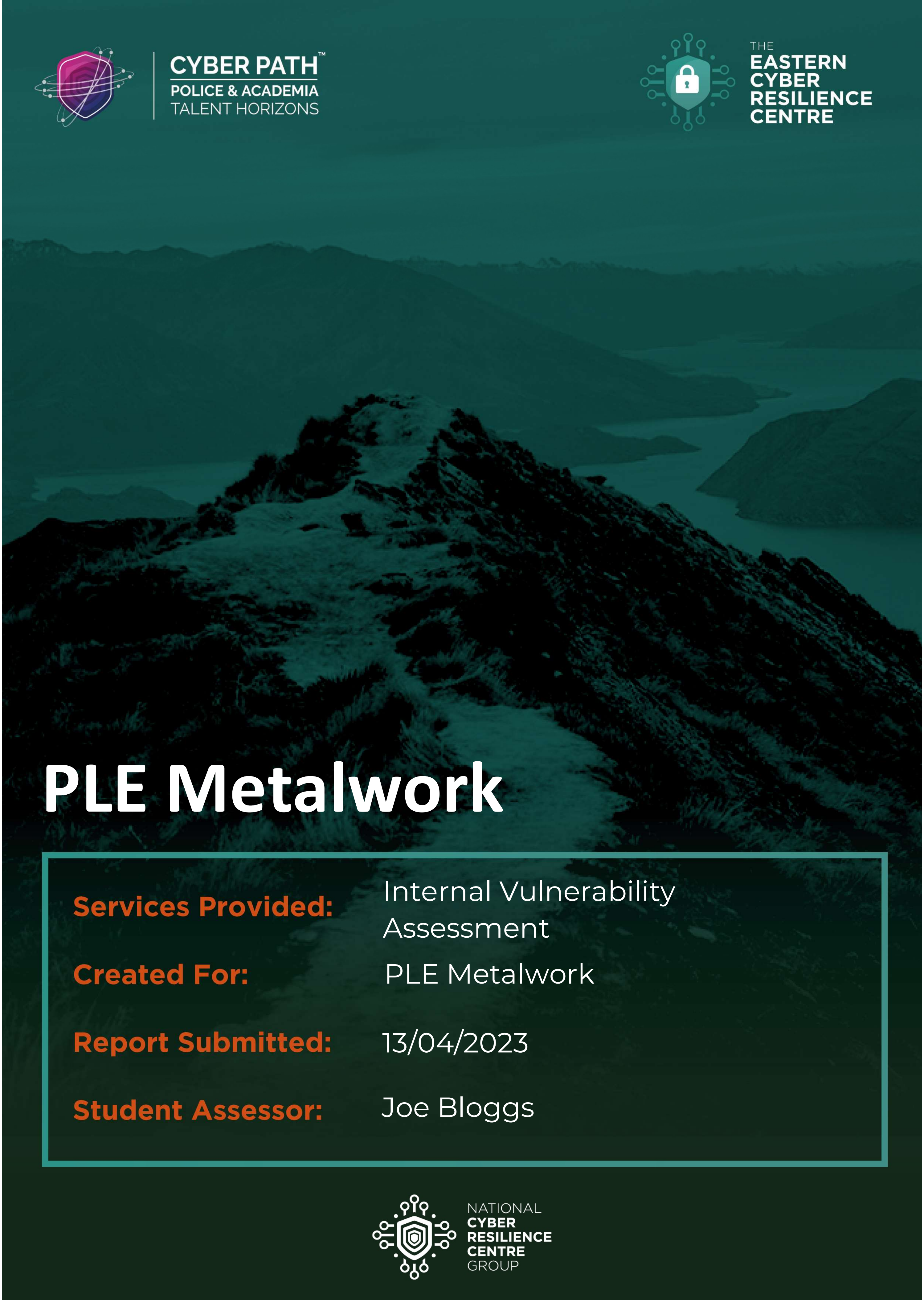


CYBER PATH™
POLICE & ACADEMIA
TALENT HORIZONS

THE
EASTERN
CYBER
RESILIENCE
CENTRE

PLE Metalwork

Services Provided:	Internal Vulnerability Assessment
Created For:	PLE Metalwork
Report Submitted:	13/04/2023
Student Assessor:	Joe Bloggs

NATIONAL
CYBER
RESILIENCE
CENTRE
GROUP

Contents

Your Assessment

Thank you for entrusting our team at the Eastern Cyber Resilience Centre to help you. Our unique partnership between Policing, Business and Academia strives to support organisations like yours on their journey to Cyber Resilience. We recognise that this may be the first time you have considered contracting a cyber service and you might be unsure what to expect or how to act on these findings. Our team are dedicated to making the process as simple and transparent as possible, to help you understand the risks highlighted in this report and how to improve on them. Please raise any questions at all with us. We are here to help you learn as much as possible – there are no silly questions here!

Assessment Information	
Service Completed	Internal Vulnerability Assessment
Assessment Completed By	Joe Bloggs
Date Completed	13/04/2023
Overseen By	Cyber PATH Student Supervisors.

Executive Summary

The executive summary identifies the key findings of the report ahead of the technical section and provides an understanding of the content of the report. This section is followed by a Risk Summary which categorises these findings into high-risk, moderate-risk, and low-risk. The technical report follows, which evidence discoveries in a way that is repeatable. The remediation and recommendation section then succinctly suggests means of removing identified information from the respective sources.

The purpose of this Internal Vulnerability Assessment was to identify misconfigurations and vulnerabilities present on the PLE Metalworks network. The assessment target scope stated that there was an originally expected 48 devices spread across 2 subnets. This executive summary serves to communicate the primary concerns that were identified in testing, used in collaboration with the risk summary and technical report to provide a clear picture to you and your technical team.

Configuration and version control of endpoints and servers is a point of interest for a large part of the report. Vulnerabilities in given software are discovered over time, and developers provide patches and updates to disable the ability to leverage those vulnerabilities for unexpected or malicious outcomes. These updates are needed for operating systems, applications, firmware, and essentially all pieces of software over a long enough time scale. Devices were found on the PLE Metalwork network that had vulnerabilities associated with them, and some devices were discovered that were far enough out of date to be classified 'End of Life', meaning that they are unable to be configured securely as the developers are no longer producing security patches. Vulnerabilities were discovered on devices running Samba, Apache, Microsoft IIS, and other software. There were similar discoveries for devices that were found to be running versions of Windows or Linux that were out of date.

Default credentials provided access to sensitive information on multiple occasions. Credentials are the combination of usernames and passwords that are used to authenticate a user for a specific service. Default credentials are installed on devices by default when they are purchased and are supposed to be changed once the devices are installed. When these credentials are unchanged it increases the threat surface of the device by providing a known set of credentials to access the device. Default credentials are shared and researchable on the internet, greatly enhancing the threat posed to these devices in the event that a person with bad intent attempts to access them. Various devices were found on the PLE Metalwork network to be using default credentials, with the most sensitive example being internal and external CCTV cameras that showed images of the physical site. A laser cutter on site, alongside internet enabled phones, were also discovered to be using default credentials.

Devices with the potential for sensitive information or impact to availability of the network need to be password protected. Multiple switches and printers were accessible in a way that suggested they could be turned off or misconfigured by the assessment team – and were not password protected. Network infrastructure was also found to have telnet enabled. Telnet is a communication protocol that facilitates remote control of devices that is insecure by nature. Further to this, plenty of unnecessary services were discovered to be running on the network, including web servers with no purpose, and file transfer servers that were configured in a way that allowed anyone to upload files to them.

This assessment was a large undertaking that has produced a lengthy technical report. This executive summary cannot summarise the findings in totality. The Eastern Cyber Resilience Centre team remains available at your convenience to discuss the findings of this report.

Risk Summary

The following table presents a summary of the risks identified throughout the assessment. It can be interpreted based on the colour and order of information. red = important and yellow=attention required. Blue= will likely not pose an ongoing threat but is worth your attention in determining if further action is required.

We would encourage you to treat all the risks and prioritise them according to our further guidance in the **Error! Reference source not found.** section. However, you may choose not to treat any of these weaknesses and accept the risks; this is an informed decision for your risk owners.

Summary of High-Risk Findings	
1	**Eternal Blue** A version of some specific software that’s present on your network is susceptible to an incredibly infamous exploit that is easily leveraged for total system control.
2	**Outdated Components** There were multiple instances of software that was running out of date on your network. Software updates serve to address identified problems and security concerns in software over time, and while it isn’t necessarily a bad thing to be out of date, it is a bad thing to have versions of software that are exposed to known vulnerabilities. This is the case on the PLE Metalwork network.
3	**Default Credentials** Default credentials are the unchanged placeholder values for usernames and passwords that come with new devices. They need to be changed as default credentials are easily discoverable from internet research. Default credentials were found on multiple devices on the network – including switches, printers, industrial hardware, and CCTV cameras.
4	**End of Life versions for multiple devices** When an operating system becomes end-of-life (EOL) it no longer receives security patches or updates from the vendor. This means that the only way to ‘patch’ this device would be by using a newer piece of hardware or software. A number of devices were discovered on the network that are likely to be EOL, and this presents a security risk to the network. Devices considered EOL were found on the network, across multiple operating systems.

Summary of Moderate-Risk Findings	
5	**Unencrypted Telnet and FTP** Software uses encryption to mathematically secure communications between users and other networked devices. The process protects against those with bad intent who could attempt to listen in on communications in what’s known as a man-in-the middle attack. Encryption scrambles data for everyone who isn’t authorised to view it, preventing this. The presence of unencrypted versions of telnet and FTP mean that there are services running

	that do not protect against these attacks. Further to this, Telnet cannot be configured securely and should never be used in a network.
6	**NT LM 0.12 SMBv1 Enabled** As discussed, SMBv1 should never be enabled on a network. It was originally used to provide shared access to files and systems – but it's now insecure and can facilitate the Eternal Blue vulnerability.

Summary of Low-Risk Findings	
7	**Misconfiguration of devices** Devices can require configuration to run as securely as possible. Devices can also arrive outdated and using default or no credentials when initially purchased. When devices are not configured correctly it can create security risks that can facilitate a person with bad intent to cause disruption or damage to the network. Devices were discovered on the network that used poor or vulnerable cryptographic security standards. Further devices were discovered that were running unencrypted services like FTP without any access control. Some devices were discovered to be running telnet, a deprecated standard for remote connection that cannot be secured.
8	**Unnecessary Services running** Cyber Security discusses the concept of a 'threat surface', which is the surface area of risk that an organisation has exposed itself to. When a service is running, it necessarily increases the 'threat surface' in that it creates more opportunities for problems and incidents. When surfaces are unnecessary, they should be shut down, as they only serve to contribute to the threat surface of the network. Examples of this were discovered in the PLE Metalwork network – including some Microsoft web servers.

Internal Vulnerability Assessment

Internal Testing

Host discovery and service enumeration are the first stage in the vulnerability assessment to map out devices on the network and the services running on them. If there are devices that are not online 24/7, this report may not be representative of all devices on the network, but rather those online during testing.

Please note the following explanations when referring to host results:

- Unresponsive; the device does not respond to typical queries and/or the ports scans are fully ignored/filtered, relative to what was found during host discovery.
- Unknown; contains ports which are difficult to attribute, therefore it cannot be ascertained what the purpose of the device is or what service it is running.

Overall Subnet Description

Table 1: List of hosts per subnet

Subnet	No. of Hosts	No. of Unresponsive	No. of Unknown
xxx.xxx.1.0/24	32	0	2
xxx.xxx.2.0/24	14	2	4

Findings of Interest

1. Unencrypted FTP Enabled
2. Unencrypted Telnet Enabled
3. Unnecessary Microsoft IIS httpd
4. Potentially EOL Linux Kernels
5. Potentially EOL Windows Versions
6. NTLM SMBv1 Enabled
7. Outdated Samba with CVEs
8. Outdated Microsoft SQL Server with CVEs
9. Insecure Cryptographic Security Standards
10. Default Credentials
11. Eternal Blue MS17-010 Vulnerability

xxx.xxx.1.0/24 Host Topology

Table 2: List of active hosts for xxx.xxx.1.0/24

IP Address	Type	Findings of Interest
xxx.xxx.1.1	Unknown Default Gateway	N/A
xxx.xxx.1.3	HiC-01 Windows 10 19041 Device	5,6,9
xxx.xxx.1.5	Hikvision IP Camera	10
xxx.xxx.1.6	Hikvision IP Camera	10
xxx.xxx.1.7	Hikvision IP Camera	10
xxx.xxx.1.10	Hikvision IP Camera	10
xxx.xxx.1.12	Hikvision IP Camera	10

xxx.xxx.1.13	Hikvision IP Camera	10
xxx.xxx.1.16	Unknown Linux Device	N/A
xxx.xxx.1.24	PLE-KT01 Kyocera TASKalfa 3252ci	1,2,9
xxx.xxx.1.25	PLE-KT03 Kyocera TASKalfa 3252ci	1,2,9
xxx.xxx.1.40	OFC-A Windows 10 17763 Device	5,6
xxx.xxx.1.41	OFC-C Windows 10 17763 Device	5,6
xxx.xxx.1.42	OFC-E Windows 10 19041 Device	5
xxx.xxx.1.44	OFC-D Windows 10 19041 Device	5
xxx.xxx.1.45	OFC-B Windows 10 17763 Device	5,6
xxx.xxx.1.65	Yealink SIP-T42U IP Phone	4,10
xxx.xxx.1.67	PLE-NAS-1 Synology Rackstation rs2421	7,9
xxx.xxx.1.70	Yealink SIP-T46S IP Phone	4
xxx.xxx.1.71	Yealink SIP-T42U IP Phone	4,10
xxx.xxx.1.72	Yealink SIP-T42U IP Phone	4,10
xxx.xxx.1.80	PLE-NAS-2 Synology Rackstation rs2421	7,9
xxx.xxx.1.82	PLE-SVR-01 Windows Server 2022 20348	3
xxx.xxx.1.84	Dell PowerEdge R710	2
xxx.xxx.1.85	PLE-DBS Windows 10 Enterprise 2015 LTSB 10240	3,8
xxx.xxx.1.86	PLE-SVR-02 Windows Server 2022 20348	3
xxx.xxx.1.87	PLE-ADM01 Windows 10 19041 Device	5
xxx.xxx.1.88	PLE-ADM03 Windows 10 19041 Device	5
xxx.xxx.1.89	PLE-ADM02 Windows 10 19041 Device	5,6
xxx.xxx.1.120	Sharp MX-2651 Printer	1,9
xxx.xxx.1.121	Sharp MX-2651 Printer	1,9
xxx.xxx.1.254	HPE ArubaOS-CX Switch	None

xxx.xxx.2.0/24 Host Topology

Table 3: List of active hosts for xxx.xxx.2.0/24

IP Address	Type	Findings of Interest
xxx.xxx.2.1	Unknown Default Gateway	N/A
xxx.xxx.2.21	Unknown Mac OS Device	N/A
xxx.xxx.2.23	Unknown Mac OS Device	N/A
xxx.xxx.2.24	Unknown Mac OS Device	N/A
xxx.xxx.2.30	DXTECH CNC Laser Cutter	2,4,10
xxx.xxx.2.31	Haas UMC-500	4
xxx.xxx.2.32	Okuma GENOS M460V-5AX	9,10
xxx.xxx.2.34	Okuma OGL 2SP-35H	1,4
xxx.xxx.2.61	Meraki MR46 WAP WR-Floor	None
xxx.xxx.2.62	Meraki MR46 WAP Zone-1	None
xxx.xxx.2.63	Meraki MR46 WAP Zone-2	None
xxx.xxx.2.254	HPE ArubaOS-CX Switch	None

Network Vulnerability Summary

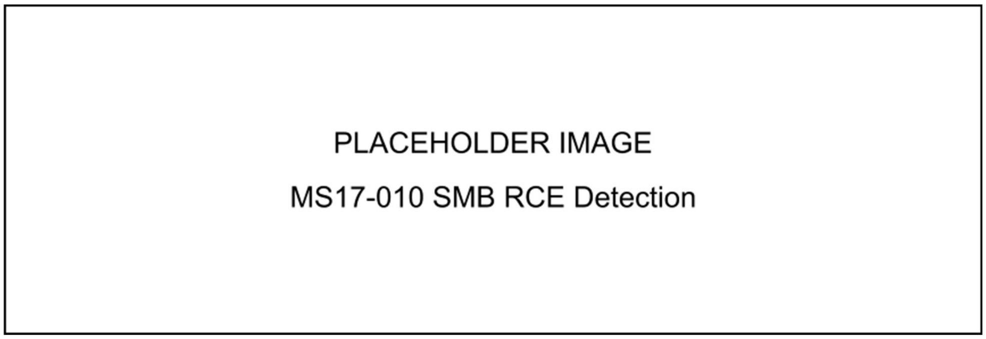
The subsections within the network vulnerability summary will break down each finding and provide relevant information in reference to the identification, vulnerability, and impact of each discovery.

Eternal Blue MS17-010 Vulnerability

EternalBlue is an exploit developed by the NSA and leaked by a hacker group in 2017. In May 2017, the infamous WannaCry ransomware virus was used to attack unpatched computers and resulted in breaches of major organisations including the NHS.

The EternalBlue vulnerability relies on the SMBv1 dialect being enabled to infect a machine. Numerous devices on the network were discovered to have SMBv1 enabled. Due to the age of SMBv1, it no longer receiving updates and numerous vulnerabilities associated with this version, Microsoft has advised customers that they should no longer using SMBv1.

A Windows 10 Enterprise 2015 LTSB 10240 device, PLE-DBS (xxx.xxx.1.85), was discovered with the SMBv1 dialect enabled and found to be vulnerable to the Eternal Blue exploit (see Figure 1).



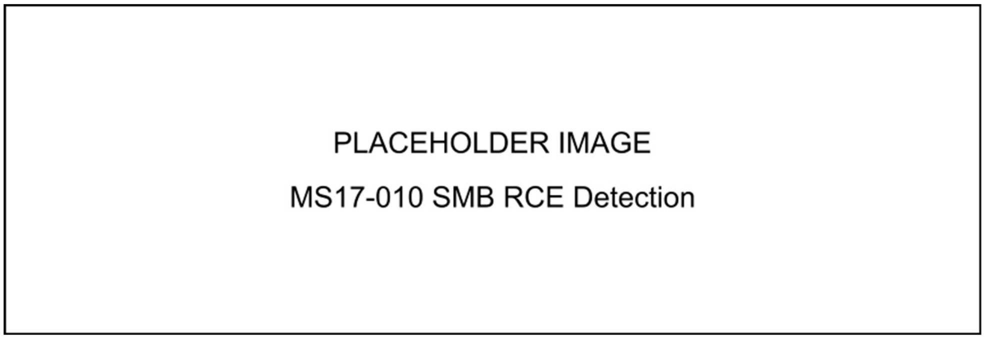


Figure 1: EternalBlue vulnerability test

Table 4 defines the CVE IDs, a unique identifier given to each vulnerability, a CVSS (version 2) score which quantifies the severity of the vulnerability on a scale of 1-10. And finally, the vulnerability type, an extract from NIST (National Institute of Standards and Technology) that provides further technical information regarding how the vulnerability works and its impact.

Table 4: EternalBlue CVE Summary

CVE	CVSS	URL	Vulnerability Type
CVE-2017-0143	9.3	https://nvd.nist.gov/vuln/detail/cve-2017-0143	Enables remote attackers to execute arbitrary code via crafted SMB packets.

Default Credentials

Default credentials are pre-defined usernames and password given to a specific device by a vender. These credentials are publicly available and are often used to allow the device to be configured upon installation. Therefore, anyone that knows the device brand/model would be able to access the device if default credentials are not changed.

Numerous devices on the network were discovered to be using default credentials. Table 5 below lists all the IP addresses/hostnames of the devices affected. Default credentials on these devices could give a person with bad intent to CCTV systems, IP Phones, and manufacturing equipment with the ability to access sensitive information and prevent access to systems.

Table 5: Default Credential Devices

IP Address	Device Type/Hostname
xxx.xxx.1.5	Hikvision IP Camera
xxx.xxx.1.6	Hikvision IP Camera
xxx.xxx.1.7	Hikvision IP Camera
xxx.xxx.1.10	Hikvision IP Camera
xxx.xxx.1.12	Hikvision IP Camera
xxx.xxx.1.13	Hikvision IP Camera
xxx.xxx.1.65	Yealink SIP-T42U IP Phone
xxx.xxx.1.71	Yealink SIP-T42U IP Phone
xxx.xxx.1.72	Yealink SIP-T42U IP Phone
xxx.xxx.2.30	DXTECH CNC Laser Cutter
xxx.xxx.2.32	Okuma GENOS M460V-5AX

Outdated Microsoft SQL Server with CVEs

Microsoft SQL Server is a Database Management System (DBMS) used for storing and retrieving data. Regular patching of servers is necessary to prevent security breaches that can compromise the confidentiality and integrity of the stored data as information on these devices can often be sensitive.

One device on the network, PLE-DBS (xxx.xxx.1.85), was discovered to be running Microsoft SQL Server 2016 with the build version "13.00.4259.00; SP1+" which was released in November 2016. This version has known vulnerabilities which are broken down in Table 6.

Table 6: Microsoft SQL CVEs

CVE	CVSSv2	URL	NVD Description
CVE-2019-1068	6.5	https://nvd.nist.gov/vuln/detail/CVE-2019-1068	A remote code execution vulnerability in Microsoft SQL

			Server which occurs when it fails to properly handle objects in memory. This can be used to execute arbitrary code in the context of the SQL Server process.
CVE-2020-0618	6.5	https://nvd.nist.gov/vuln/detail/CVE-2020-0618	A remote code execution vulnerability which exists in the Microsoft SQL Server Reporting Services when it fails to sanitize input. This can be used to execute arbitrary code in the context of the Report Server service account
CVE-2021-1636	6.5	https://nvd.nist.gov/vuln/detail/CVE-2021-1636	An exploit that allows an elevation of privilege within Microsoft SQL.
CVE-2016-7249	6.5	https://nvd.nist.gov/vuln/detail/CVE-2016-7249	This is an exploit that allows remote authenticated users to elevate their privileges within the system
CVE-2016-7250	6.5	https://nvd.nist.gov/vuln/detail/CVE-2016-7250	This allows an elevation of privilege to authenticated users allowing them to run commands that usually cannot be run.
CVE-2022-29143	6.0	https://nvd.nist.gov/vuln/detail/CVE-2022-29143	Microsoft SQL Server Remote Code Execution Vulnerability.
CVE-2017-8516	5.0	https://nvd.nist.gov/vuln/detail/CVE-2017-8516	Allows for an information disclosure vulnerability when it improperly enforces permissions, aka "Microsoft SQL Server Analysis Services Information Disclosure Vulnerability".
CVE-2016-7251	4.3	https://nvd.nist.gov/vuln/detail/CVE-2016-7251	Cross-site scripting (XSS) vulnerability in the MDS API in Microsoft SQL Server 2016 allows remote attackers to inject arbitrary web script or HTML via an unspecified parameter, aka "MDS API XSS Vulnerability."
CVE-2016-7252	4.0	https://nvd.nist.gov/vuln/detail/CVE-2016-7252	Microsoft SQL Server 2016 mishandles the FILESTREAM path, which allows remote authenticated users to gain privileges via unspecified vectors, aka "SQL Analysis Services Information Disclosure Vulnerability."

Outdated Samba with CVEs

Samba is an open-source software suite that enables file and printer sharing between Unix/Linux-based systems and Windows-based systems. It allows Unix and Linux-based systems to act as file servers, print servers, and authentication servers for Windows-based clients, providing seamless integration between different operating systems.

Two Synology NAS (network attached storage) devices had 40 separate vulnerabilities associated with Samba 4.6.2 – the outdated version that it is running. These vulnerabilities range in severity, with the most severe vulnerabilities allowing remote attackers to execute code on the device. Table 8 defines the CVE IDs, and type of vulnerabilities that were identified for this version of Samba. Table 7 defines the two devices affected by this vulnerable service.

Table 7: Devices with Outdated Samba

IP Address	Device Type / Hostname
xxx.xxx.1.67	PLE-NAS-1 Synology Rackstation rs2421
xxx.xxx.1.80	PLE-NAS-2 Synology Rackstation rs2421

Table 8: Outdated Samba CVEs

CVE	CVSS	URL	Vulnerability Type
CVE-2017-7494	10.0	https://nvd.nist.gov/vuln/detail/CVE-2017-7494	Allows remote attackers to execute code.
CVE-2020-25719	9.0	https://nvd.nist.gov/vuln/detail/CVE-2020-25719	Allows local users to achieve total domain compromise.
CVE-2020-17049	9.0	https://nvd.nist.gov/vuln/detail/CVE-2020-17049	Allows attackers to bypass security features to gain access.
CVE-2022-32744	8.8	https://nvd.nist.gov/vuln/detail/CVE-2022-32744	Allows local users to change other users' passwords, enabling full domain takeover.
CVE-2022-0336	8.8	https://nvd.nist.gov/vuln/detail/CVE-2022-0336	Allows remote attackers to cause a denial of service, intercept traffic and impersonate existing services.
CVE-2020-25717	8.5	https://nvd.nist.gov/vuln/detail/CVE-2020-25717	Allows an authenticated attacker to escalate privileges.
CVE-2020-10745	7.8	https://nvd.nist.gov/vuln/detail/CVE-2020-10745	Allows remote attackers to cause a denial of service.
CVE-2017-14746	7.5	https://nvd.nist.gov/vuln/detail/CVE-2017-14746	Allows remote attackers to execute arbitrary code.
CVE-2017-11103	6.8	https://nvd.nist.gov/vuln/detail/CVE-2017-11103	Allows remote attackers to impersonate services and potentially launch other attacks.
CVE-2021-3738	6.5	https://nvd.nist.gov/vuln/detail/CVE-2021-3738	Allows remote attackers to cause a denial of service or potentially escalate privileges.
CVE-2020-25722	6.5	https://nvd.nist.gov/vuln/detail/CVE-2020-25722	Allows attackers to achieve total domain compromise.

CVE-2020-25718	6.5	https://nvd.nist.gov/vuln/detail/CVE-2020-25718	Allows attackers to escalate privileges.
CVE-2018-10858	6.5	https://nvd.nist.gov/vuln/detail/CVE-2018-10858	Allows remote attackers to execute arbitrary code on Samba clients.
CVE-2018-1057	6.5	https://nvd.nist.gov/vuln/detail/CVE-2018-1057	Allows authenticated users to change other users’ passwords, including administrative users and privileged accounts (e.g., Domain Controllers).
CVE-2019-14870	6.4	https://nvd.nist.gov/vuln/detail/CVE-2019-14870	Allows remote attackers to impersonate services and potentially launch other attacks.
CVE-2017-12151	5.8	https://nvd.nist.gov/vuln/detail/CVE-2017-12151	Allows remote attackers to read or alter a Samba connection through a man-in-the-middle attack.
CVE-2017-12150	5.8	https://nvd.nist.gov/vuln/detail/CVE-2017-12150	Allows remote attackers to read a Samba connection through a man-in-the-middle attack.
CVE-2019-3880	5.5	https://nvd.nist.gov/vuln/detail/CVE-2019-3880	Allows remote attackers to create files in Samba shares.
CVE-2019-14902	5.5	https://nvd.nist.gov/vuln/detail/CVE-2019-14902	Allows authenticated users to modify Domain Controller subtrees, even after losing rights to do so.
CVE-2022-32746	5.4	https://nvd.nist.gov/vuln/detail/CVE-2022-32746	Allows authenticated attackers to use improperly allocated memory in a use-after-free attack, potentially causing a denial of service or executing arbitrary code.
CVE-2021-20277	5.0	https://nvd.nist.gov/vuln/detail/CVE-2021-20277	Allows remote attackers to cause a denial of service.
CVE-2020-27840	5.0	https://nvd.nist.gov/vuln/detail/CVE-2020-27840	Allows remote attackers to cause a denial of service.
CVE-2020-10704	5.0	https://nvd.nist.gov/vuln/detail/CVE-2020-10704	Allows remote attackers to cause a denial of service.
CVE-2017-15275	5.0	https://nvd.nist.gov/vuln/detail/CVE-2017-15275	Allows remote attackers to obtain sensitive information in improperly allocated memory.
CVE-2021-20254	4.9	https://nvd.nist.gov/vuln/detail/CVE-2021-20254	Allows remote attackers to obtain sensitive information about user accounts in improperly allocated memory.
CVE-2019-14833	4.9	https://nvd.nist.gov/vuln/detail/CVE-2019-14833	Allows users to create weak passwords by failing to check password complexity, making them vulnerable to password attacks.

CVE-2017-12163	4.8	https://nvd.nist.gov/vuln/detail/CVE-2017-12163	Allows remote attackers to obtain sensitive information from server memory.
CVE-2016-2124	4.3	https://nvd.nist.gov/vuln/detail/CVE-2016-2124	Allows remote attackers to intercept plaintext passwords, even with Kerberos authentication.
CVE-2020-14383	4.0	https://nvd.nist.gov/vuln/detail/CVE-2020-14383	Allows authenticated attackers cause a denial of service, resulting in some services not restarting upon reboot.
CVE-2020-14318	4.0	https://nvd.nist.gov/vuln/detail/CVE-2020-14318	Allows authenticated attackers to obtain certain file and directory information.
CVE-2020-10760	4.0	https://nvd.nist.gov/vuln/detail/CVE-2020-10760	Allows authenticated attackers to cause a denial of service in a use-after-free attack.
CVE-2020-10730	4.0	https://nvd.nist.gov/vuln/detail/CVE-2020-10730	Allows authenticated users to potentially perform a use-after-free attack or exploit a NULL pointer dereference, likely causing a denial of service.
CVE-2019-14847	4.0	https://nvd.nist.gov/vuln/detail/CVE-2019-14847	Allows remote attackers to cause a denial of service.
CVE-2018-16851	4.0	https://nvd.nist.gov/vuln/detail/CVE-2018-16851	Allows authenticated attackers to cause a denial of service due to NULL pointer dereferencing.
CVE-2018-16841	4.0	https://nvd.nist.gov/vuln/detail/CVE-2018-16841	Allows remote attackers to cause a denial of service when Samba is configured to accept smart-card authentication.
CVE-2018-14629	4.0	https://nvd.nist.gov/vuln/detail/CVE-2018-14629	Allows local attackers to cause a denial of service.
CVE-2018-10919	4.0	https://nvd.nist.gov/vuln/detail/CVE-2018-10919	Allows authenticated attackers to obtain sensitive information.
CVE-2019-14861	3.5	https://nvd.nist.gov/vuln/detail/CVE-2019-14861	Allows authenticated attackers to create new DNS records and potentially cause a denial of service.
CVE-2018-1050	3.3	https://nvd.nist.gov/vuln/detail/CVE-2018-1050	Allows remote attackers to cause a denial of service.
CVE-2020-14323	2.1	https://nvd.nist.gov/vuln/detail/CVE-2020-14323	Allows local attackers to cause a denial of service.

Configuration Review

This section covers the configuration of applications and appliances throughout the network, and the consequent findings by the assessment team.

Each subsection will explain the findings that the assessment team has determined could either widen the attack surface or reduce overall network resilience.

NT LM 0.12 SMBv1 Enabled

Server Message Block (SMB) is a protocol used for communication over networks, often in relation to file systems and sharing. Since the initial 1.0 release in 1996 there have been numerous changes and improvements to better the functionality and security of the protocol.

The most notorious security incident relating to *SMB* in recent years was the WannaCry ransomware attacks in 2017. The SMBv1 protocol was exploited to spread and infect devices with ransomware worldwide.

Microsoft has advised customers to stop using SMBv1 because of the number of vulnerabilities associated with it. Devices were discovered on the network that were using SMBv1, and these are available in Table 9.

Table 9: Devices with SMBv1 Enabled

IP Address	Device Name
xxx.xxx.1.3	HiC-01 Windows 10 19041 Device
xxx.xxx.1.40	OFC-A Windows 10 17763 Device
xxx.xxx.1.41	OFC-C Windows 10 17763 Device
xxx.xxx.1.45	OFC-B Windows 10 17763 Device
xxx.xxx.1.89	PLE-ADM02 Windows 10 19041 Device

Insecure Cryptographic Security Standards

Cryptography plays a critical role in securing network communication by using mathematical algorithms to transform information into an unreadable form for anyone without the proper key. This technique is essential to safeguard sensitive data such as passwords, financial information, and personal data from being intercepted and read by unauthorized parties. The fundamental principle behind cryptography is to ensure that only authorized parties have access to the information being transmitted by encrypting the data, making it indecipherable to anyone who lacks the decryption key. This approach guarantees that even if an attacker gains access to the encrypted data, they cannot read it without the decryption key, making it a vital tool in network security.

However, as computational power continues to increase, the strength of cryptographic algorithms can become compromised over time. As computing power grows, it becomes easier for attackers to break the encryption and access the sensitive information being transmitted.

To ensure that cryptography remains effective, it is important to regularly maintain and update the cryptographic algorithms being used. This includes updating key lengths, implementing new algorithms, and retiring algorithms that are no longer considered secure.

Diffie-Hellman Key Exchange

The Diffie-Hellman key exchange is a cryptographic protocol that allows two parties to securely exchange cryptographic keys over an insecure channel. The keys generated through this protocol can be used for encryption and decryption of messages, as well as for other purposes in cryptography – and is used on the PLE network.

The protocol relies on the use of a mathematical concept that makes it difficult for an attacker to determine the keys being exchanged by the two parties – If the 'strength of the group' used in the Diffie-Hellman key exchange is too short, it can be vulnerable to attacks. The strength of the group is determined by the length of the prime number used in the protocol. If the prime number is too short, it can be easily factored (or 'guessed') by an attacker, allowing them to determine the keys being exchanged.

The ideal length for the prime number used in the Diffie-Hellman key exchange depends on the level of security required but - as of 2021, it is recommended to use a minimum key length of 2048 bits for the prime number. This provides a strong level of security against attacks.

If the prime number used is too short, it can be easily factored using a simple computer, allowing a person with bad intent to determine the keys being exchanged. This can lead to the compromise of the encrypted messages and any other information that relies on the security of the keys. This would be possible on some machines discovered on the network, which are detailed in **Error! Reference source not found.** below.

IP Address	Device Name
xxx.xxx.1.3	HiC-01 Windows 10 19041 Device
xxx.xxx.1.24	PLE-KT01 Kyocera TASKalfa 3252ci
xxx.xxx.1.25	PLE-KT03 Kyocera TASKalfa 3252ci
xxx.xxx.1.67	PLE-NAS-1 Synology Rackstation rs2421
xxx.xxx.1.80	PLE-NAS-2 Synology Rackstation rs2421
xxx.xxx.1.120	Sharp MX-2651 Printer
xxx.xxx.1.121	Sharp MX-2651 Printer
xxx.xxx.2.32	Okuma GENOS M460V-5AX

Potentially EOL Linux Kernels

The Linux Kernel is the core component of any Linux distribution and is the operative interface between hardware and software. Like any operating system or piece of software, new vulnerabilities are discovered over time. Whilst this is not usually a problem for general purpose systems due to the ease of updating and patching the Kernel, embedded devices do not share this ability.

The difficulties of updating the Kernel as well as software dependency issues can result in embedded and IoT devices becoming neglected and easily surpassing their EOL dates.

XX is a demonstration of how multiple Linux Kernels on embedded devices on the network have likely exceeded their EOL.

Table 10: Linux Kernel EOL

IP	Linux Kernel	Device Type	EOL
xxx.xxx.1.65	2.6.32	Yealink SIP-T42U IP Phone	March 2016
xxx.xxx.1.70	3.2.102	Yealink SIP-T46S IP Phone	May 2018
xxx.xxx.1.71	2.6.32	Yealink SIP-T42U IP Phone	March 2016
xxx.xxx.1.72	2.6.32	Yealink SIP-T42U IP Phone	March 2016

xxx.xxx.2.30	4.3*	DXTECH CNC Laser Cutter	February 2016
xxx.xxx.2.31	3.14	Haas UMC-500	August 2016

* OS fingerprinting was unable to determine an exact Linux Kernel version. Version numbers of each of the devices should be ascertained to conclude whether the device Kernels are EOL.

Potentially Outdated Windows Versions

Updates from vendors such as Microsoft often include fixes for bugs, performance and most importantly, vulnerabilities. When vulnerabilities are discovered in software, security patches are released to address and resolve them.

When an operating system becomes end-of-life (EOL) it no longer receives security patches or updates from the vendor. This means that the only way to patch a device would be by using a newer piece of hardware or software. A number of devices were discovered on the network that are likely to be EOL. These Windows machines were running versions between 1709 and 1909, with the former declared EOL in October 2020, and the latter in May 2022. They are detailed in **Error! Reference source not found.**.

Table 11: Devices with likely EOL Windows Versions.

IP Address	Device Name	Version	End-of-life GAC / LTSC
xxx.xxx.1.3	HiC-01	Windows 10 19041 2004	December 14, 2021 / None
xxx.xxx.1.40	OFC-A	Windows 10 17763 Redstone 5	November 10, 2020 / January 9, 2029
xxx.xxx.1.41	OFC-C	Windows 10 17763 Redstone 5	November 10, 2020 / January 9, 2029
xxx.xxx.1.42	OFC-E	Windows 10 19041 2004	December 14, 2021 / None
xxx.xxx.1.44	OFC-D	Windows 10 19041 2004	December 14, 2021 / None
xxx.xxx.1.45	OFC-B	Windows 10 17763 Redstone 5	November 10, 2020 / January 9, 2029
xxx.xxx.1.87	PLE-ADM01	Windows 10 19041 2004	December 14, 2021 / None
xxx.xxx.1.88	PLE-ADM03	Windows 10 19041 2004	December 14, 2021 / None
xxx.xxx.1.89	PLE-ADM02	Windows 10 19041 2004	December 14, 2021 / None

*Some end dates vary depending on edition

Table 12: GAC & LTSC Editions

General Availability Channel (GAC)		Long-Term Servicing Channel (LTSC)
Home, Pro, Pro Education, Pro for Workstations	Education, Enterprise, IoT Enterprise	Enterprise, IoT Enterprise

Unencrypted Telnet Enabled

Telnet is a protocol that enables two systems to communicate with each other bidirectionally. However, Telnet transmits data over the network without encryption, making it inherently vulnerable to man-in-the-middle (MITM) attacks, including password sniffing. Attackers can exploit this vulnerability to intercept and read sensitive data transmitted over Telnet connections. As a result, Telnet should not be used for transmitting sensitive data over unsecured networks, and alternative secure protocols such as SSH should be utilized to ensure confidentiality and integrity of network communications.

Multiple devices on the network were discovered to be running unencrypted Telnet services as seen in Table 13.

Table 13: Devices with Telnet Enabled

IP Address	Device Type/Hostname
xxx.xxx.1.24	PLE-KT01 Kyocera TASKalfa 3252ci
xxx.xxx.1.25	PLE-KT03 Kyocera TASKalfa 3252ci
xxx.xxx.2.30	DXTECH CNC Laser Cutter

Unencrypted FTP Enabled

FTP (File Transfer Protocol) is a protocol used to transfer files between computer systems on a network. It does not utilise any security mechanisms, so transferred data is sent in plaintext without any encryp5tion. This means FTP communications are susceptible to being intercepted through a *man-in-the-middle attack*.

Numerous printers and other networked machinery were discovered to be running the FTP service on port 22 Table 14 below lists all these devices.

Table 14: Devices with FTP Enabled

IP Address	Device Type/Hostname
xxx.xxx.1.24	PLE-KT01 Kyocera TASKalfa 3252ci
xxx.xxx.1.25	PLE-KT03 Kyocera TASKalfa 3252ci
xxx.xxx.1.120	Sharp MX-2651 Printer
xxx.xxx.1.121	Sharp MX-2651 Printer
xxx.xxx.2.34	Okuma OGL 2SP-35H

Transmitting sensitive information over FTP, such as sending a document to a printer, could be intercepted by a person with bad intent. Depending on the information intercepted, this could be used in a range of attacks including data breaches or cyber extortion. Furthermore, login credentials sent over FTP could be intercepted in a password sniffing attack.

Unnecessary Microsoft IIS httpd

Two Windows Server 2022 devices (PLE-SVR-01 & PLE-SVR-02) were discovered to be running Microsoft IIS httpd 10.0 with the default landing page. Whilst this web server does not have any known vulnerabilities; keeping services like this running unnecessarily increases the likelihood of a vulnerability being present. Hence why disabling it would contribute towards network hardening and a reduced attack surface.

Table 15 below lists the two aforementioned devices.

Table 15: Devices running Microsoft IIS httpd

IP Address	Device Type/Hostname
xxx.xxx.1.82	PLE-SVR-01 Windows Server 2022 20348
xxx.xxx.1.86	PLE-SVR-02 Windows Server 2022 20348

Risk Prioritization

This following section will briefly outline the order of risk prioritization by weighing the risks of each vulnerability found on the network.

1) Eternal Blue MS17-010 Vulnerability

A Windows 10 Enterprise 2015 LTSB 10240 device, PLE-DBS (xxx.xxx.1.85), was found to be susceptible to the Eternal Blue MS17-010 (CVE-2017-0143) vulnerability. The device is a crucial component of the PLE network, as it contains the Microsoft SQL Server. Since the vulnerability could lead to remote code execution on the device, it is considered a high-risk issue. Therefore, it is recommended to apply immediate mitigation measures as outlined in the Mitigation Proposal.

2) Outdated Samba with CVEs

Two network attached storage devices were found to be running Samba version 4.6.2. This particular version of Samba has been associated with 40 CVEs, ranging from denial-of-service attacks to remote code execution. Given the severity and the high number of vulnerabilities present, it is strongly recommended to apply immediate mitigation measures as suggested in the Mitigation Proposal.

3) Outdated Microsoft SQL Server with CVEs

One device on the network was identified, namely PLE-DBS (xxx.xxx.1.85), to be operating Microsoft SQL Server 2016, with the build version "13.00.4259.00; SP1+." This version of SQL Server is outdated and has known vulnerabilities. The most recent service pack available for this version of SQL Server was released in September 2021. Given the severity of the vulnerabilities, it is highly recommended to take immediate remedial action, as suggested in the Mitigation Proposal.

4) Default Credentials

The use of default credentials was found to be a common issue across the network and appeared in various scenarios. Access was often granted to web interfaces on devices like IP phones, CCTV cameras, and embedded systems on manufacturing equipment. Since default credentials are easily discoverable online, this poses a significant risk to the overall network security and integrity. Therefore, it is advised to implement mitigation measures to address this issue.

5) NTLM SMBv1 Enabled

SMBv1, also known as Server Message Block version 1, is a network protocol used for network file sharing on Windows operating systems. However, due to its outdated nature and previous security issues it is recommended to follow the advice presented in the Mitigation Proposal.

6) Unencrypted FTP Enabled

FTP, or File Transfer Protocol, is an unencrypted protocol that was discovered to be enabled on numerous devices. However, due to its lack of encryption, attackers can intercept data transmitted over FTP, including login credentials and documents sent to printers. This interception could potentially result in the disclosure of sensitive information or the provision of privileged login credentials to attackers. To address this issue, we recommend reviewing the Mitigation Proposal.

7) Potentially EOL Linux Kernels & Windows Versions

Once an operating system reaches its end-of-life (EOL), it no longer receives security patches or updates from the vendor. This makes it impossible to patch a device except by installing newer hardware or software. During our assessment, we identified several devices on the network that are likely to have reached EOL. To address the security risks associated with using unsupported devices, we strongly recommend remediating the identified devices in accordance with the Mitigation Proposal.

8) Unencrypted Telnet Enabled

Telnet is enabled on a significant number of devices, making it possible for attackers to intercept unencrypted data transmitted over the protocol, including login credentials and commands issued to devices like switches. Such interception can provide attackers with access to sensitive information related to system configurations and privileged login credentials. To prevent such security breaches, we advise referencing the Mitigation Proposal.

9) Unnecessary Microsoft IIS httpd

Two devices on the network were found to be unnecessarily running Microsoft IIS httpd with the default landing page enabled. Whilst this web server version has no known CVEs it is important to remove any unnecessary services as part of network hardening measures to reduce the attack surface.

There’s more to the Eastern Cyber Resilience Centre…

There are many additional ways to engage with ECRC. If you haven’t already, you can register as a Core Member of the Eastern community, which is free of charge. This membership includes practical, government-approved guidance, as well as regular information updates to keep you informed of our other help and services on offer, including:

- **Educational Events** - we run regular webinars and events on a range of topics relevant to your small business or third sector organisation
- **Affordable solutions** - we offer a range of paid services like this one which are designed to address the most pertinent risks affecting SMEs, as identified by policing and Government.
- **Cyber Essentials Certification** - we have a Cyber Essentials Partners forum, which is made up of IASME approved Cyber Essentials Certifiers. If you are planning on achieving Cyber Essentials or Cyber Essentials Plus certification, we can refer you to the Cyber Essentials Partners forum of local suppliers in the region that provide this.

About the Cyber Resilience Centre Network

The National Cyber Resilience Centre Group and Cyber Resilience Centres are funded and supported by the Home Office and policing in a not-for-profit partnership with the private sector and academia to strengthen our national cyber resilience across SMEs and the supply chain.

At a national level, NCRCG is building a coalition of police, government, large employers and organisations, and academia to ensure a collaborative and coherent approach to cyber resilience. NCRCG and its National Ambassadors and the CRC network are committed to investing in the next generation of cyber experts. As such, NCRCG has launched Cyber PATH in partnership with the CRC network and over 45 universities.

The nine CRCs operate across England and Wales. They serve SMEs in their locality helping to build cyber resilience against threats that are specific to them. Cyber PATH empowers students to work with their regional CRC in meeting the requests brought to them by local businesses.

Each CRC retains the freedoms to deliver tailored, trusted and affordable support, with NCRCG providing insight and solutions at a macro level.

You can learn more about the work of the NCRCG here. We can help your own customers and suppliers too, so spread the word.

Help Bundles and Additional Services

If you are ready for more support, we offer free Core membership and a selection of Help Bundles which include paid services and 12 months of support. This includes:

- Full website vulnerability testing
- Policy Review
- Staff awareness training
- And more....

Visit our selection of Help Bundles and Services here.

You can also engage with us through our social media channels – find us on LinkedIn, Twitter and Facebook.

Get in touch with us at enquiries@ecrcentre.co.uk if there’s anything else we can help you with.