CYBER PATH
POLICE & ACADEMIA
TALENT HORIZONS

THE
CYBER
RESILIENCE
CENTRE
NETWORK

XXX

Services Provided: External Vulnerability Assessment

Created for: Engineering Ltd

Report Submitted: 03/01/2026

Student Assessor: Alex Thomas

Contents

Your Assessment

Thank you for entrusting our team at Cyber PATH 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	External Vulnerability Assessment
Assessment Completed By	Student Joe Bloggs
Date Completed	14/12/2025
Overseen By	Cyber PATH supervisor Abdullah Khan

Executive Summary

This executive summary intends to present the potential key risks that our team collated from the recent assessment service that we were entrusted to deliver for you. This report is presented in two sections.

- Executive Summary / Risk Summary – included for your risk focused, senior stakeholders who may not have a technical background.

- Technical Detail – an incredibly detailed and informative capture of all our team's work and output. This section is intended for your technical audience who may be involved in the mitigation.

External Vulnerability Assessment

On this service delivery, our team remotely assesses your organisations connection point to the internet, the virtual main door of your organisation that can be regularly knocked upon by any number of anonymous internet users. The risk profile of such internet-connected systems could describe as significant, as anyone connected to the internet can attempt to interact with your virtual door. It's not uncommon for organisation to present services via the connection point such as email, a company portal or remote access technology. Each service could be likened to a letterbox, a small window into your organisation's internal environment.

Our team did not note any significant findings from the assessment of your organisation's external point of connection however, we would suggest that all potential future configuration changes are carefully considered, and risk assessed.

Thank you

We are truly grateful to have been entrusted in providing these services to you. Our team's focus is very much on presenting risk as a basis for further internal discussion. We hope that the following risk position and subsequent detailed technical report will provide a clear position on our findings. We are of course here at your convenience should you or your team have further questions or wish to explore the points we have raised in our work for you.

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.

.

Summary of High-Risk Findings	
1	**Default Credentials.** Default credentials are the unchanged values for usernames and passwords that are programmed on devices when they arrive from the manufacturers. 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 printers, IP phones and power management cards.
2	**Vulnerable outdated /End-of-Life (EOL) software.** As time passes, new vulnerabilities within software are identified. This can be by researchers or potentially those with bad intent. These vulnerabilities are fixed and released to users by means of software updates/patches. Each software version has a life cycle and once the software version is retired by the manufacturers, they may choose to continue to support the software for a limited period. After this period has lapsed no further updates/patches are released for that software version, making treatment for any vulnerabilities discovered after that date difficult. Manufacturers of the software expect that a user will either accept the risk of using the vulnerable software or upgrade to a newer edition. Several devices were discovered on the network that ran Windows Server 2016, which is End of Life as of 11th January 2022. Two device running Windows Server 2019, approaching its End of Life in January 2024, were also discovered. Across the network, it was identified that outdated software with known vulnerabilities were being used. This software included Microsoft SQL Servers, gSoap, CUPS and OpenSSH.

Summary of Moderate-Risk Findings	
4	**SMBv1 enabled and message signing disabled.** Server Message Block (SMB) is a network file-sharing protocol used by Windows for sharing files, printers, and other resources between devices on a network. SMBv1 is a weak protocol and was exploited to spread the WannaCry ransomware. SMBv1 has been a deprecated protocol as of 2014. It is encouraged to move away from SMBv1 as the default protocol and use the more secure SMBv2 and SMBv3. Three devices on the network had SMBv1 enabled and set as default.
5	**Unencrypted FTP with anonymous login** 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 is known as a man-in-the-middle attack. Encryption obfuscates the data for everyone who is not authorised to view it, preventing this attack. The presence of unencrypted versions of FTP on the network means that this service does not protect against these attacks. Further to this, devices on the network with FTP enabled had a default feature enabled called anonymous login. This allows a user to connect to the server without providing a specific username or password. Instead, the user can use the credentials anonymous/anonymous to gain access to the FTP server.
6	**Unencrypted Telnet with anonymous login** Telnet is the foundational protocol allowing devices to connect over the Internet. Telnet transmits data over the network in plain text without encryption, making it inherently vulnerable to man-in-the-middle (MITM) attacks. A person with bad intent can exploit this vulnerability to intercept and read sensitive data transmitted over Telnet connections. For this reason, Telnet should never be used in a network. Devices across the assessment had the Telnet protocol running and furthermore connection to Telnet for some devices was gained without the need for any means of authentication. No username or password was required to connect to the network via Telnet.

There were no low-risk findings.

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.

Vulnerabilities in software are uncovered over time and are assigned a unique identifier called a CVE, which stands for Common Vulnerabilities and Exposures. CVEs are considered known vulnerabilities due to the formal process used to assess the vulnerability before it is assigned a CVE number along with a severity score (CVSS), which is between 1 and 10, with 10 being the most severe. Unknown vulnerabilities are weaknesses or flaws within a piece of software that are not yet formally identified. Each CVE mentioned within this report is linked to the vulnerability on NIST's National Vulnerability Database (NVD), which is a repository of CVEs and can provide more details. Throughout this document the CVSS scoring metrics used is the updated version, CVSSv3, unless it is stated otherwise (CVSSv2). Version 3 of the CVSS provides a more comprehensive and accurate assessment of the vulnerability as it offers a more detailed and customisable approach to scoring than its predecessor.

Overall Subnet Description

Table 1: List of hosts per subnet

Subnet	No. of Hosts	No. of Unresponsive	No. of Unknown
xxx.xxx.15.0/24	24	2	2
xxx.xxx.16.0/24	73	0	9
xxx.xxx.18.0/24	24	0	19
xxx.xxx.19.0/24	3	2	1
xxx.xxx.90.0/24	3	0	2

Findings of Interest List

Below is a list of the discoveries made during the assessment of the network. Each discovery has been assigned a unique number. The host topology, which follows after this list, displays the corresponding number(s) for each device.

1 Default Credential Access
2 Outdated SSH with CVEs
3 Outdated SQL Server with CVEs
4 Outdated Samba with CVEs

xxx.xxx.15.0/24 Host Topology

Table 2: List of active hosts for xxx.xxx.15.0/24

IP Address	Hostname (xxx.xxx.local) / Device	Findings of Interest
xxx.xxx.15.1	IP camera	11, 15, 17
xxx.xxx.15.2	HikVision IP Camera	15, 17
xxx.xxx.15.3	HikVision IP Camera	15, 17
xxx.xxx.15.4	UNV IPC3634ER3-DPZ28 IP Camera	11, 15, 17
xxx.xxx.15.5	IP Camera	2, 11, 15, 17
xxx.xxx.15.6	HikVision IP Camera	12, 15
xxx.xxx.15.7	Herospeed IP Camera	12, 15, 17
xxx.xxx.15.8	Herospeed IP Camera	12
xxx.xxx.15.9	Herospeed IP Camera	12
xxx.xxx.15.10	Herospeed IP Camera	12, 15, 17
xxx.xxx.15.11	Herospeed IP Camera	12, 15, 17
xxx.xxx.15.12	HikVision IP Camera	12
xxx.xxx.15.13	HikVision IP Camera	12
xxx.xxx.15.14	HikVision IP Camera	12
xxx.xxx.15.15	HikVision IP Camera	12
xxx.xxx.15.16	HikVision IP Camera	12
xxx.xxx.15.17	HikVision IP Camera	12
xxx.xxx.15.18	HikVision IP Camera	12
xxx.xxx.15.19	HikVision IP Camera	12
xxx.xxx.15.111	HikVision IP Camera	12, 15
xxx.xxx.15.112	-	15
xxx.xxx.15.113	-	15
xxx.xxx.15.150	LThomas2 / PowerChute	-
xxx.xxx.15.254	Linksys WRT45G	15

xxx.xxx.16.0/24 Host Topology

Table 3: List of active hosts for xxx.xxx.16.0/24

IP Address	Hostname (xxx.xxx.local) / Device	Findings of Interest
xxx.xxx.16.1	Comms / Windows Server 2016	8, 10, 11, 13
xxx.xxx.16.3	Rdserver / Windows Server 2016	13
xxx.xxx.16.6	Nl-Newt-Print / Windows Server 2019	14
xxx.xxx.16.8	Nl-Newt-DC02 / Windows Server 2019	14
xxx.xxx.16.9	DCServer2016 / Windows Server 2016	13
xxx.xxx.16.11	Fileserver-02 / Windows Server 2016	13
xxx.xxx.16.12	TW-Remoteaccess / Windows Server 2016	7, 13
xxx.xxx.16.13	Radius / Windows Server 2016	13
xxx.xxx.16.16	Sageserver / SQL Server	3, 10, 11
xxx.xxx.16.17	XXX-DR2	3, 4, 12, 15
xxx.xxx.16.18	Zynk-Server / Windows Server 2016	10, 11, 13
xxx.xxx.16.19	Devzynk / Windows Server 2016	13
xxx.xxx.16.22	Laptop-AR / Windows 11	-
xxx.xxx.16.23	WH3	-
xxx.xxx.16.24	Boardroom	-
xxx.xxx.16.25	S-Wiggins	3
xxx.xxx.16.30	Andy-WH	-
xxx.xxx.16.33	Laptop-CT	-
xxx.xxx.16.36	WH2	13
xxx.xxx.16.39	Netgear GS724T Switch	15
xxx.xxx.16.41	Scatterick	13
xxx.xxx.16.42	Netgear GS724T Switch	15
xxx.xxx.16.45	Pspicer-VM / Windows Server 2016	7
xxx.xxx.16.46	ZA1137027996 / EcoStruxure	12, 16
xxx.xxx.16.47	ZA1808022842 / EcoStruxure	1, 12, 16
xxx.xxx.16.48	EcoStruxure	16
xxx.xxx.16.50	Pcphiluses-Nloffice	13, 16
xxx.xxx.16.52	Xxx.xxx-DR2	4, 15
xxx.xxx.16.58	Xxx.xxx-DR2	4, 15
xxx.xxx.16.62	SBrown	-
xxx.xxx.16.63	Kgreenway	13
xxx.xxx.16.86	A-King / Windows 11	-
xxx.xxx.16.87	Lthomas2 / Windows 10	-
xxx.xxx.16.96	Mash2	-
xxx.xxx.16.101	C458L / Konica Minolta BizHub C458 Printer	1, 15, 16
xxx.xxx.16.102	C458M / Konica Minolta Biz Hub C458 Printer	1, 15, 16
xxx.xxx.16.104	Printer	15
xxx.xxx.16.106	Printer	-
xxx.xxx.16.107	Datamax 4606 Printer	1, 11
xxx.xxx.16.108	Printer	-
xxx.xxx.16.109	Brother MFC-7360N Printer	8

xxx.xxx.16.110	Printer	-
xxx.xxx.16.111	HikVision Camera	12
xxx.xxx.16.113	RM_NG / Zebra ZTC GK420d Printer	1, 8, 9, 11
xxx.xxx.16.114	RM_WH2 / Zebra ZTC GK420d Printer	1, 8, 9, 11
xxx.xxx.16.115	RM_WH1 / Zebra ZTC GK420d Printer	1, 8, 9, 11
xxx.xxx.16.116	Royal Mail – IT / Zebra ZTC ZD421-230dpi ZPL Printer	1, 8, 9, 11
xxx.xxx.16.124	WH1	-
xxx.xxx.16.151	VMware ESXi Host Client	-
xxx.xxx.16.154	Skyline-Photon-Machine/ VMware Skyline Collector	2, 16
xxx.xxx.16.156	Vcentre / VMware VSphere	2
xxx.xxx.16.157	VM-NAS / Netgrear ReadyNAS	6, 16
xxx.xxx.16.159	VM-NAS / Netgrear ReadyNAS	6, 16
xxx.xxx.16.160	Fujitsu iRMC S5 Web Server	2, 16
xxx.xxx.16.161	VMware ESXi Host Client	-
xxx.xxx.16.174	Netgear GS105Ev2 Switch	12
xxx.xxx.16.230	NL-NEWT-UPSSHUTDOWN / PowerChute	-
xxx.xxx.16.231	UPSSHUTDOWN / PowerChute	2
xxx.xxx.16.237	iqn.2022-09.Phil-NAS / NAS	5
xxx.xxx.16.238	Netgear GS105Ev2 Switch	12
xxx.xxx.16.239	Netgear GS105Ev2 Switch	11
xxx.xxx.16.241	Netgear GS105Ev2 Switch	11
xxx.xxx.16.242	VPN	15
xxx.xxx.16.244	VPN	15
xxx.xxx.16.245	Netgear GS752TPS Switch	12, 15
xxx.xxx.16.246	Netgear GS752TPS Switch	12, 15
xxx.xxx.16.247	Netgear GS752TPS Switch	12, 15
xxx.xxx.16.248	Netgear GS748T Switch	15
xxx.xxx.16.249	Netgear GS748T Switch	15
xxx.xxx.16.250	Netgear GS724T Switch	15
xxx.xxx.16.251	Netgear GS724T Switch	15
xxx.xxx.16.252	Netgear GS748T Switch	15
xxx.xxx.16.253	Netgear GS724T Switch	15

xxx.xxx.18.0/24 Host Topology

Table 4: List of active hosts for xxx.xxx.18.0/24

IP Address	Hostname (xxx.xxx.local) / Device	Findings of Interest
xxx.xxx.18.51	-	-
xxx.xxx.18.53	Boardroomnl.xxx.xxx.2 / VoIP	1, 12
xxx.xxx.18.54	Xxx.xxxboardroomphone.xxx.xxx / VoIP	1, 12
xxx.xxx.18.55	-	-
xxx.xxx.18.57	-	-

xxx.xxx.18.58	-	-
xxx.xxx.18.59	-	-
xxx.xxx.18.60	-	-
xxx.xxx.18.61	-	-
xxx.xxx.18.62	-	-
xxx.xxx.18.65	-	-
xxx.xxx.18.72	-	-
xxx.xxx.18.76	-	-
xxx.xxx.18.77	-	-
xxx.xxx.18.81	-	-
xxx.xxx.18.100	Gigaset-N720-DM-PRO / Gigaset N720 DM Pro	1
xxx.xxx.18.101	-	-
xxx.xxx.18.102	-	-
xxx.xxx.18.103	-	-
xxx.xxx.18.104	-	-
xxx.xxx.18.106	-	-
xxx.xxx.18.107	-	-
xxx.xxx.18.108	Ngfax.xxx.xxx.2 / Grandstream HT701	1, 9
xxx.xxx.18.254	Sophos Firewall / Linksys WRT45G	15

xxx.xxx.19.0/24 Host Topology

Table 5: List of active hosts for xxx.xxx.19.0/24

IP Address	Hostname (xxx.xxx.local) / Device	Findings of Interest
xxx.xxx.19.100	Cyberoam Router/Firewall	15

xxx.xxx.90.0/24 Host Topology

Table 6: List of active hosts for xxx.xxx.19.0/24

IP Address	Hostname (xxx.xxx.local) / Device	Findings of Interest
xxx.xxx.90.16	-	2
xxx.xxx.90.17	-	2
xxx.xxx.90.253	Linksys WRT45G	15

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.

Default Credentials Access

Default credentials are pre-defined usernames and password combinations given to devices from the manufacturer. These credentials are used for installation and can be discovered online. A person with bad intent who knows the device brand/model would be able to search for these credentials and attempt to use them to gain access to the device if they have yet to be changed.

Several devices on the networks assessed were discovered to be using their respective default credentials. Table 7 below lists all the IP addresses/Device names of the devices affected along with their default credentials. Screenshots where default credentials were used to gain access can be seen in Figure 1 & Figure 2.

Table 7: List of devices with default credentials

IP Address	Device Name / Device	Credentials (username/password)
xxx.xxx.16.47	ZA1808022842 / EcoStruxure	device/apc
xxx.xxx.16.101	C458L / Konica Minolta BizHub C458 Printer	Direct Access
xxx.xxx.16.102	C458M / Konica Minolta Biz Hub C458 Printer	Direct Access
xxx.xxx.16.107	Datamax 4606 / Printer	Direct Access
xxx.xxx.16.113	RM_NG / Zebra ZTC GK420d Printer	admin/1234
xxx.xxx.16.114	RM_WH2 / Zebra ZTC GK420d Printer	admin/1234
xxx.xxx.16.115	RM_WH1 / Zebra ZTC GK420d Printer	admin/1234
xxx.xxx.16.116	Royal Mail – IT / Zebra ZTC ZD421-230dpi ZPL Printer	Direct Access
xxx.xxx.18.53	Boardroomnl.xxx.xxx.2 / Yealink W60B	admin/admin
xxx.xxx.18.54	Xxx.xxxboardroomphone.xxx.xxx / Yealink W60B	admin/admin
xxx.xxx.18.100	Gigaset-N720-DM-PRO / Gigaset N720 DM Pro	-/admin
xxx.xxx.18.108	Ngfax.xxx.xxx.2 / Grandstream HT701	-/admin

Figure 1: Default credentials to access XX on xxx.xxx.16.47

Figure 2: Default credentials to printer on xxx.xxx.16.113

Outdated SSH with CVEs

SSH (Secure Shell) is a communication protocol that allows network devices to securely communicate over a network. It is commonly used for remote access to machines. Regular patching is necessary to plug the holes/vulnerabilities discovered within the software over time. This will ensure these services are not misused or abused by attackers exploiting known vulnerabilities. SSH versions can use different cryptographic protocols for security, certain protocols provide better encryption standards and, in turn, more secure transmissions.

Several versions of SSH were present across the networks assessed. Table 8 shows the versions with CVEs identified and the corresponding IP addresses. Due to the vast numbers of CVEs for the SSH version identified, a limited number have been shown. The NIST website can identify all known vulnerabilities associated with the versions identified. Table 9 shows the CVEs and which version of SSH they apply to.

Table 8: Devices and SSH versions

IP Address	Device Name/ Device	SSH Type/Version
xxx.xxx.15.5	IP Camera	OpenSSH 6.2
xxx.xxx.16.154	Skyline-Photon-Machine/ VMware Skyline Collector	OpenSSH 7.8
xxx.xxx.16.156	Vcentre / VMware VSphere	OpenSSH 7.8
xxx.xxx.16.160	Fujitsu iRMC S5 Web Server	OpenSSH 7.4p1
xxx.xxx.16.231	UPSSHUTDOWN / PowerChute	OpenSSH 8.0
xxx.xxx.90.16	-	OpenSSH 8.9p1
xxx.xxx.90.17	-	OpenSSH 8.9p1

Table 9: SSH versions and CVE list

CVE	CVSSv3	OpenSSH Versions	NVD Description
CVE-2023-28531	9.8	OpenSSH 8.9p1	SSH-Add in OpenSSH adds smartcard keys to ssh-agent without the intended per-hop destination constraints.
CVE-2015-5600	8.5 CVSSv2	OpenSSH 6.2	Remote attackers can conduct brute force attacks or cause denial of service.
CVE-2019-16905	7.8	OpenSSH 7.8	Memory corruption and local code execution through an integer overflow if the client/server is configured to uses XMSS key.
CVE-2014-1692	7.5 CVSSv2	OpenSSH 6.2	Allow remote attackers to cause a denial of service via memory corruption.
CVE-2021-28041	7.1	OpenSSH 8.9p1 OpenSSH 8.4p1	SSH-agent has a double free which leads to the same memory address location being allocated and the program's memory management data structures becoming corrupted leading to buffer overflow attacks.

CVE-2021-41617	7.0	OpenSSH 7.4p1 OpenSSH 7.8 OpenSSH 8.0 OpenSSH 8.4p1	Allows privilege escalation when non-default configurations are used, as supplemental groups are not initialised.
CVE-2019-6110	6.8	OpenSSH 7.4p1 OpenSSH 7.8	A man-in-the-middle attack (malicious server) can manipulate the client output, which is due to accepting and displaying arbitrary stderr output from the server.
CVE-2019-6109	6.8	OpenSSH 7.4p1 OpenSSH 7.8	A man-in-the-middle attack (malicious server) can employ cradted object names to manipulate the client output, which is due to missing character encoding in the progress display.
CVE-2020-14145	5.9	OpenSSH 7.4p1 OpenSSH 7.8 OpenSSH 8.0 OpenSSH 8.4p1	An attacker can perform a man-in-the-middle attack to target initial connection attempts (where no host key for the server has been cached by the client).
CVE-2018-15919	5.3	OpenSSH 7.4p1 OpenSSH 7.8	Remotely observable behaviour in auth.gss2.c could let an attacker detect the existence of users on a system.
CVE-2018-15473	5.3	OpenSSH 7.4p1	Allows for user enumeration vulnerability
CVE-2017-15906	5.3	OpenSSH 7.4p1	Does not prevent write operations in readonly mode. This is through the process_open function in sftp-server.c.

Outdated SQL Server with CVEs

SQL Servers are a Database Management System (DBMS) used for storing and retrieving data. Regular patching of servers is necessary to stop these vulnerabilities discovered within the software being abused.

Two versions of SQL Servers were present on the networks assessed. Table 10 shows the servers found which have CVEs, along with where they were located.

Table 10: SQL server devices and versions

IP Address	Hostname (xxx.xxx.local)	SQL Server Version
xxx.xxx.16.16	SXXX	MySQL 5.0.40-enterprise-nt / Microsoft SQL Server 2019 15.00.2101.00; GDR1+
xxx.xxx.16.17	Xxx.xxx-DR2	MySQL 5.0.40-enterprise-nt / Microsoft SQL Server 2019 15.00.2101.00; GDR1+
xxx.xxx.16.25	SXXX	MySQL 5.0.40-enterprise-nt

Table 11 lists the CVE identified for the discovered SQL server versions and CVSSv3 scores with a brief description of the vulnerability (sourced from NIST). Due to the range of CVEs found, the list is not exhaustive but shows the key issues with each version respectively. As some versions have not been assigned CVSSv3 scores, CVSSv2 scores are provided and detailed where appropriate.

Table 11: CVE listing for SQL server versions.

SQL Server Version Affected	CVE	CVSSv3	NVD Description
Microsoft SQL Server 2019 15.00.2101.00; GDR1+	CVE-2023-38169	8.8	Remote code execution vulnerability
	CVE-2023-21713	8.8	Remote code execution vulnerability
	CVE-2023-21705	8.8	Remote code execution vulnerability
	CVE-2021-1636	8.8	Elevation of privilege vulnerability
	CVE-2023-32028	7.8	Remote code execution vulnerability
	CVE-2023-32027	7.8	SQL Server remote code execution vulnerability
	CVE-2023-32026	7.8	SQL Server remote code execution vulnerability
	CVE-2023-32025	7.8	SQL Server remote code execution vulnerability
	CVE-2023-29356	7.8	SQL Server remote code execution vulnerability
	CVE-2023-29349	7.8	Remote code execution vulnerability
	CVE-2023-21718	7.8	SQL Server remote code execution vulnerability
	CVE-2022-29143	7.5	SQL Server remote code execution vulnerability
	CVE-2023-23384	7.3	SQL Server remote code execution vulnerability
MySQL 5.0.40-enterprise-nt	CVE-2009-0819	4.0 CVSSv2	Allows for remotely authenticated users to cause a denial of service.
	CVE-2007-5925	4.0 CVSSv2	Allows for remotely authenticated users to cause a denial of service.

Outdated Samba with CVEs

Samba is a suite of software that builds upon the SMB protocol, which provides access to shared resources like file shares and network-connected printers.

The XXX network has 3 devices running Samba version 4.6.2 which is an outdated version. This version of Samba has 44 separate vulnerabilities associated. These vulnerabilities range in severity, with the most severe vulnerabilities (shown below) allowing remote attackers to execute code on a device. The devices which have Samba 4.6.2 running on it are shown in Table 12 along with their IP location. Table 13 defines the CVE IDs, and type of vulnerabilities that were identified for this version of Samba.

Table 12: Devices identified as running vulnerable version of Samba

IP Address	Host/Device Name
xxx.xxx.16.17	Xxx.xxx-DR2
xxx.xxx.16.52	Xxx.xxx-DR2
xxx.xxx.16.58	Xxx.xxx-DR2

Table 13: CVE listing for Samba version 4.6.2

CVE	CVSSv3	NVD Description
CVE-2017-7494	9.8	Allows remote attackers to execute arbitrary code.
CVE-2017-14746	9.8	Allows remote attackers to execute arbitrary code.
CVE-2022-32744	8.8	Full domain takeover by encrypting forged kpasswd requests, a user can change other users' passwords.
CVE-2021-3738	8.8	Denial of service or privileged escalation
CVE-2020-25722	8.8	Full domain compromise due to multiple flaws in the Samba AD DC access and conformance checking.
CVE-2018-10858	8.8	Allows remote attackers to execute arbitrary code via a heap-buffer overflow.
CVE-2018-1057	8.8	Privilege escalation as authenticated users can change any other users' password due to the Samba AD DC incorrectly validates permission to modify passwords.
CVE-2020-25717	8.1	Privilege escalation flaw found in the way Samba maps domain users to local users.
CVE-2020-10745	7.5	Denial of service attack whereby a remote attacker can cause the Samba server to consume excessive CPU use.
CVE-2020-17049	7.2	Kerberos security feature bypass vulnerability

Outdated CUPS with CVEs

The 'Common Unix Printing System' – or CUPS, is a system that allows a device to become a print server and manage printing jobs over a given network. It can be used to queue, filter, and schedule printing, among other features. CUPS was found to be installed on a Network Attached Storage device (xxx.xxx.16.237) and may be used to facilitate a networked print server on this endpoint.

Updates are released to keep the software up to date and to remediate vulnerabilities discovered in previous versions. The version of CUPS found on the Network Attached Storage device (1.1) is considered outdated. The relevant CVEs for this vulnerable version of CUPS are discussed in Table 14 (sourced from NIST).

Table 14: CVEs affecting CUPS Version 1.1

CVE	CVSSv2	NVD Description
CVE-2008-5184	10.0	The web interface uses the guest username when a user is not logged on to the web server. This makes it easier for remote attackers to bypass intended policy and conduct Cross Site Request Forgery attacks.
CVE-2008-0053	10.0	Multiple buffer overflows might allow remote attackers to execute arbitrary code.
CVE-2007-4351	10.0	Off-by-one error in the ippReadIO function allows for a denial of service.
CVE-2010-2941	7.9	Ipp.c does not allocate memory properly which can lead a remote attacker to cause a denial of service or possibly execute arbitrary code.
CVE-2009-1182	7.5	Multiple buffer overflows might allow remote attackers to execute arbitrary code.
CVE-2008-3639	7.5	Heap-based buffer overflow allows remote attackers to execute arbitrary code.
CVE-2009-1180	6.8	Allows remote attackers to execute arbitrary code via a crafted PDF file.
CVE-2009-1179	6.8	An integer overflow allows remote attackers to execute arbitrary code via a crafted PDF file.
CVE-2009-0163	6.8	Denial of service or execution of arbitrary code via a crafted TIFF image.
CVE-2009-0164	6.4	Remote attacks can conduct DNS rebinding attack as the web interface for CUPS does not validate the HTTP Host header in the client request.

Outdated Netatalk with CVEs

Netatalk is a free, open-source implementation of the Apple Filing Protocol (AFP). It allows Linux based operating systems to serve as file servers for Macintosh computers (MacOS). Netatalk is integrated into a range of NAS solutions such as the Netgear ReadyNAS devices found on the network at xxx.xxx.16.157 & xxx.xxx.16.159.

Updates are released to keep the software up to date and to remediate vulnerabilities discovered in previous versions. The version of Netatalk found on the Network Attached Storage device, 3.1.12, is considered outdated. The relevant CVEs for this vulnerable version of Netatalk are discussed in Table 15 (sourced from NIST).

Table 15: CVE listing for Netatalk version 3.1.12

CVE	CVSSv3	NVD Description
CVE-2023-42464	9.8	A Type Confusion vulnerability was found in the Spotlight RPC functions. Due to a lack of type checking in callers of the dalloc_value_for_key() function, a malicious actor may be able to fully control the value of the pointer and theoretically achieve Remote Code Execution on the host.
CVE-2022-23125	9.8	A remote attacker can execute arbitrary code without being authenticated.
CVE-2022-23124	9.8	A remote attacker can disclose sensitive information without being authenticated.
CVE-2022-23123	9.8	A remote attacker can disclose sensitive information without being authenticated.
CVE-2022-23122	9.8	A remote attacker can execute arbitrary code without being authenticated.
CVE-2022-23121	9.8	A remote attacker can execute arbitrary code without being authenticated.
CVE-2018-1160	9.8	A remote attacker can execute arbitrary code without being authenticated.
CVE-2022-45188	7.8	Heap-based buffer overflow will result in code execution via a crafted .appl file. Which could result in remote root access on some platforms.

Outdated gSoap with CVEs

gSOAP is a toolkit used during software development in relation to the processing of XML which is a data type. Like all software, gSOAP requires security patches and updates to fix vulnerabilities discovered by the community over time. Several devices were discovered on the network to be running a vulnerable version of gSOAP.

The affected devices and the relevant versions of gSOAP are listed in Table 16; the CVEs and descriptions are shown in Table 17 (sourced from NIST).

Table 16: Devices running outdated versions of gSOAP

IP Address	Device Name	gSOAP Version
10.10.15.1	IP Camera	2.7
xxx.xxx.15.2	HikVision IP Camera	2.8
xxx.xxx.15.3	HikVision IP Camera	2.8
xxx.xxx.15.4	UNV IPC3634ER3-DPZ28 IP Camera	2.7
xxx.xxx.15.5	IP Camera	2.8
xxx.xxx.15.7	Herospeed IP Camera	2.8
xxx.xxx.15.10	Herospeed IP Camera	2.8
xxx.xxx.15.11	Herospeed IP Camera	2.8

Table 17: gSOAP version 2.7 & 2.8 CVEs list

CVE	*CVSSv3*	*NVD Description*
CVE-2019-7659	8.1	Allows attackers to cause a denial of service (application abort) or possibly have unspecified other impact
CVE-2017-9765	8.1	Allows remote attackers to execute arbitrary code or cause a denial of service (stack-based buffer overflow and application crash) via a large XML document

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. SMBv1 is a protocol which has been deprecated since 2014.

The most prominent 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 its number of associated vulnerabilities. Devices were discovered on the network that were using SMBv1, and these are available in Table 18.

Table 18: Devices with SMBv1 Enabled

IP Address	Hostname / Device
xxx.xxx.16.12	TW-Remoteaccess
xxx.xxx.16.45	Pspicer-VM
xxx.xxx.16.159	VM-NAS / Netgear ReadyNAS

Unencrypted FTP Enabled with Default Credentials

File Transfer Protocol (FTP) is a protocol used to transfer files between computer systems on a network. It does not use any security mechanisms and sends data unencrypted by default. This means FTP communications are susceptible to being intercepted through a man-in-the-middle attack and at risk of manipulating the data being sent and received. The widely adopted alternative is Secure File Transfer Protocol (SFTP), as FTP should only be restricted to closed devices and trusted environments.

Several printers and other networked devices were discovered to be running the FTP service. These devices were also discovered to be using default or anonymous credentials for FTP, which would allow a perpetrator to connect to those systems.

Default credentials are easily found online, such as anonymous login. Anonymous login (username: anonymous and password: anonymous) are accepted without any validation and gives access to the FTP server. A list of affected devices is listed in (Table 19) and a screenshot of access to the FTP server using anonymous login in Figure 3.

Table 19: Devices running FTP protocol

IP Address	Hostname (xxx.xxx.local) / Device
xxx.xxx.16.1	Comms / Linksys WRT45G
xxx.xxx.16.109	Brother MFC-7360N Printer
xxx.xxx.16.113	RM_NG / Zebra ZTC GK420d Printer
xxx.xxx.16.114	RM_WH2 / Zebra ZTC GK420d Printer
xxx.xxx.16.115	RM_WH1 / Zebra ZTC GK420d Printer
xxx.xxx.16.116	Royal Mail – IT / Zebra ZTC ZD421-230dpi ZPL Printer

Figure 3: FTP anonymous login for xxx.xxx.16.1

Unencrypted Telnet Enabled with Default Credentials

Telnet is a protocol that enables two systems to communicate with each other bidirectionally. Telnet transmits data over the network in plain text 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 data over a network.

Devices on the network were identified to be running unencrypted telnet services, and in addition these devices were discovered to be using telnet with default credentials. The devices are shown in the table below (Table 20) along with a screenshot of access to one of those devices shown in Figure 4.

Table 20: Devices running Telnet protocol

IP Address	Device Name
xxx.xxx.16.113	RM_NG / Zebra ZTC GK420d Printer
xxx.xxx.16.114	RM_WH2 / Zebra ZTC GK420d Printer
xxx.xxx.16.115	RM_WH1 / Zebra ZTC GK420d Printer
xxx.xxx.16.116	Royal Mail – IT / Zebra ZTC ZD421-230dpi ZPL Printer
xxx.xxx.18.108	Ngfax.xxx.xxx.2 / Grandstream HT701

Figure 4: Telnet access using default credentials for device on xxx.xxx.18.80

Default Web Server Running

Three devices were discovered to be running Microsoft IIS httpd 10.0 with the default IIS landing page. Whilst this version of Microsoft IIS does not have any known vulnerabilities; keeping services like this running unnecessarily increases the possible attack surface of the device. Table 21 below lists the two affected devices.

Table 21: Devices running the default web server.

IP Address	Hostname (xxx.xxx.local)/Device
xxx.xxx.16.1	Comms / Linksys WRT45G
xxx.xxx.16.16	Sageserver
xxx.xxx.16.18	Zynk-Server

Self-Signed TLS/SSL Certificate

Certification can be achieved from a Certificate Authority (CA) but can also be achieved using self-certification. Self-certified certificates do not expire. If encryption standards fall out of date, no prompted remediation process will be offered in the same way that a Certificate Authority-issued certification would provide.

If a private key is exposed, then the lack of ability to revoke the certificate will complicate the remediation of the incident. Self-signed certificates may also warn end users that the site they are using is not secure. If trained to ignore these warnings, end users may ignore them when they find these warnings during normal business practise. Devices with self-signed TLS/SSL certificates are presented in Table 22.

Table 22: Device running self-signed TLS/SSL Certificates

IP Address	Hostname (xxx.xxx.local)/Device
xxx.xxx.16.46	ZA1137027996 / EcoStruxure
xxx.xxx.16.47	ZA1808022842 / EcoStruxure
xxx.xxx.16.48	EcoStruxure
xxx.xxx.16.50	Pcphiluses-Nloffice
xxx.xxx.16.101	C458L / Konica Minolta BizHub C458 Printer
xxx.xxx.16.102	C458M / Konica Minolta Biz Hub C458 Printer
xxx.xxx.16.154	Skyline-Photon-Machine/ VMware Skyline Collector
xxx.xxx.16.157	VM-NAS / Netgrear ReadyNAS
xxx.xxx.16.159	VM-NAS / Netgrear ReadyNAS
xxx.xxx.16.160	Fujitsu iRMC S5 Web Server

No HTTPS Enabled

Hypertext Transfer Protocol (HTTP) is the foundational mechanism through which computers

interact with websites to retrieve and display web content. Communication over HTTP is done without encryption, meaning any communication is easily visible to anyone listening on the network. The need for security has led to the Hypertext Transfer Protocol Secure (HTTPS). This protocol provides a secure layer for web communication meaning that any communication over this protocol is encrypted, and only the intended recipient can read the communication.

Enabling HTTPS for exclusively internal IP addresses is important because it can help to protect the confidentiality and integrity of data transmitted over the network.

Even if the device has an HTTP service that is exclusively internal, there is still the potential for a person with bad intent to intercept or modify network traffic – which could be used to steal sensitive information like login credentials, personal data, or confidential business information. With HTTPS, data is encrypted before it is transmitted over the network and decrypted only by the intended recipient. This makes it much more difficult for attackers to eavesdrop on or modify network traffic.

Devices were discovered on the network that did not have HTTPS enabled and were therefore communicating unencrypted using HTTP. These are detailed in Table 23.

Table 23: Devices which do not have HTTPS enabled.

IP Address	Device Name
xxx.xxx.15.1	IP camera
xxx.xxx.15.4	UNV IPC3634ER3-DPZ28 IP Camera
xxx.xxx.15.5	IP Camera
xxx.xxx.16.1	Comms / Linksys WRT45G
xxx.xxx.16.16	Sageserver
xxx.xxx.16.18	Zynk-Server
xxx.xxx.16.107	Datamax 4606 Printer
xxx.xxx.16.113	RM_NG / Zebra ZTC GK420d Printer
xxx.xxx.16.114	RM_WH2 / Zebra ZTC GK420d Printer
xxx.xxx.16.115	RM_WH1 / Zebra ZTC GK420d Printer
xxx.xxx.16.116	Royal Mail – IT / Zebra ZTC ZD421-230dpi ZPL Printer
xxx.xxx.16.239	/ Netgear GS105Ev2 Switch
xxx.xxx.16.241	/ Netgear GS105Ev2 Switch

HTTP not redirecting to HTTPS

HTTP (Hypertext Transfer Protocol) is used to transmit hypermedia - documents such as HTML, between a sender and receiver. It is most used to communicate between web browsers and servers. HTTPS (Hypertext Transfer Protocol Secure) uses TLS encryption to maintain the privacy and integrity of data in transit.

Web servers typically use port 80 and port 443. When an HTTP request is sent to port 80, they are typically redirected and upgraded to HTTPS on port 443. When this does not happen, an insecure

connection is made to the web server, which provides an opportunity for a person with bad intent to intercept communications in a man-in-the-middle attack. Whilst ports 80 and 443 are standard, some web servers often use higher port ranges to avoid conflict if multiple web servers are running.

Devices which do not redirect to the HTTPS version are shown in Table 24 below.

Table 24: Devices which do not direct port 80 traffic to the secure HTTPS port.

IP Address	Device Name
xxx.xxx.15.6	HikVision IP Camera
xxx.xxx.15.7	Herospeed IP Camera
xxx.xxx.15.8	Herospeed IP Camera
xxx.xxx.15.9	Herospeed IP Camera
xxx.xxx.15.10	Herospeed IP Camera
xxx.xxx.15.11	Herospeed IP Camera
xxx.xxx.15.12	HikVision IP Camera
xxx.xxx.15.13	HikVision IP Camera
xxx.xxx.15.14	HikVision IP Camera
xxx.xxx.15.15	HikVision IP Camera
xxx.xxx.15.16	HikVision IP Camera
xxx.xxx.15.17	HikVision IP Camera
xxx.xxx.15.18	HikVision IP Camera
xxx.xxx.15.19	HikVision IP Camera
xxx.xxx.15.111	HikVision IP Camera
xxx.xxx.16.17	Xxx.xxx-DR2
xxx.xxx.16.46	ZA1137027996 / EcoStruxure
xxx.xxx.16.47	ZA1808022842 / EcoStruxure
xxx.xxx.16.111	/ HikVision Camera
xxx.xxx.16.174	/ Netgear GS105Ev2 Switch
xxx.xxx.16.238	/ Netgear GS105Ev2 Switch
xxx.xxx.16.245	/ Netgear GS752TPS Switch
xxx.xxx.16.246	/ Netgear GS752TPS Switch
xxx.xxx.16.247	/ Netgear GS752TPS Switch
xxx.xxx.18.53	Boardroomnl.xxx.xxx.2 / VoIP
xxx.xxx.18.54	Xxx.xxxboardroomphone.xxx.xxx / VoIP

Likely EOL Windows Version

Updates from vendors such as Microsoft often include fixes for bugs, performance issues, 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.

It is recommended to manually assess and verify Windows versions in use in the XXX network, as fingerprinting is not accurate enough to give actionable information. Table 25 shows which devices on the network are believed to have exceeded their EOL however these will need to be manually confirmed.

Table 25: Device with EOL Windows version

IP Address	Hostname	Version	Date of EOL
xxx.xxx.16.1	COMMS	Windows Server 2016	11th Jan 2022
xxx.xxx.16.3	RDSERVER	Windows Server 2016	11th Jan 2022
xxx.xxx.16.9	DCServer2016	Windows Server 2016	11th Jan 2022
xxx.xxx.16.11	Fileserver-02	Windows Server 2016	11th Jan 2022
xxx.xxx.16.12	TW-Remoteaccess	Windows Server 2016	11th Jan 2022
xxx.xxx.16.13	Radius	Windows Server 2016	11th Jan 2022
xxx.xxx.16.18	Zynk-Server	Windows Server 2016	11th Jan 2022
xxx.xxx.16.19	Devzynk	Windows Server 2016	11th Jan 2022
xxx.xxx.16.36	WH2	Windows XP Service pack 3	8th April 2014
xxx.xxx.16.41	MASH2	Windows XP Service pack 3	8th April 2014
xxx.xxx.16.50	PCPHILUSES-NLOFFICE	Windows XP Service pack 3	8th April 2014
xxx.xxx.16.63	KGreenway	Windows XP Service pack 3	8th April 2014

Approaching Windows EOL Date

As previously mentioned in the EOL Windows & Linux Kernel section, once a product is classified as EOL by its vendor, it will no longer receive security updates or patches which could put the device at risk.

Devices on the network were discovered to be running Windows Server 2019 (Table 26), which will become EOL as of the 9th of January 2024.

Table 26: Windows Device Approaching EOL

IP Address	Hostname
xxx.xxx.16.6	NL-NEWT-PRINT
xxx.xxx.16.8	NL-NEWT-DC02

Likely EOL Linux Kernel

Embedded and Internet of Things (IoT) devices are often Linux-based due to various reasons that make it an appealing environment for developers. The Linux Kernel is the core component of any Linux distribution and is the primary interface between hardware and processes.

Like any operating system, vulnerabilities are discovered over time that drives patching and new versions of the software being released. This means that older versions of the Linux Kernel have known vulnerabilities that can be exploited. 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 and software dependency issues can result in embedded and IoT devices becoming neglected and easily surpassing their EOL dates. It is worthwhile understanding the presence of Linux Kernels on your network and manually confirming what version they are running. It is recommended to manually assess and verify Linux Kernels in use in the XXX network, as fingerprinting is not accurate enough to give actionable information. Table 27 shows which devices on the network are believed to have exceeded their EOL however these will need to be manually confirmed.

Table 27 - Devices that have potentially reached EOL and should have their kernel versions manually verified.

IP Address	Device Name	Fingerprinted Kernel Version	End Of Life Date
xxx.xxx.15.1	IP Camera	Linux 2.6.32 – 3.13	Mar 2016 –Apr 2014
xxx.xxx.15.2	HikVision IP Camera	Linux 3.10	Nov 2017
xxx.xxx.15.3	HikVision IP Camera	Linux 3.10	Nov 2017
xxx.xxx.15.4	IP Camera	Linux 3.4.35	Oct 2016
xxx.xxx.15.5	IP Camera	Linux 2.6.32 – 3.13	Mar 2016 –Apr 2014
xxx.xxx.15.6	HikVision IP Camera	Linux 3.10 – 4.11	Nov 2017 – Jul 2017
xxx.xxx.15.7	Herospeed IP Camera	Linux 2.6.32 – 3.13	Mar 2016 –Apr 2014
xxx.xxx.15.10	Herospeed IP Camera	Linux 3.10 – 4.11	Nov 2017 – Jul 2017
xxx.xxx.15.11	Herospeed IP Camera	Linux 3.10 – 4.11	Nov 2017 – Jul 2017
xxx.xxx.15.111	HikVision IP Camera	Linux 2.6.32 – 3.13	Mar 2016 –Apr 2014
xxx.xxx.15.112	-	Linux 2.6.32 – 3.13	Mar 2016 –Apr 2014
xxx.xxx.15.113	-	Linux 2.6.32 – 3.13	Mar 2016 –Apr 2014
xxx.xxx.15.254	Router	Linux 3.10	Nov 2017
xxx.xxx.16.17	XXX-DR2	Linux 2.6.32 – 4.4	Mar 2016 – Jan 2027
xxx.xxx.16.39	Netgear GS724T Switch	Linux 2.6.32 - 3.13	Mar 2016 –Apr 2014
xxx.xxx.16.42	Netgear GS724T Switch	Linux 2.6.32 - 3.13	Mar 2016 –Apr 2014
xxx.xxx.16.52	XXX-DR2	Linux 2.6.32 – 4.4	Mar 2016 – Jan 2027
xxx.xxx.16.58	XXX-DR2	Linux 2.6.32 – 4.4	Mar 2016 – Jan 2027
xxx.xxx.16.101	C458L / Printer	Linux 3.2 - 3.8	May 2018 – May 2013
xxx.xxx.16.102	C458M / Printer	Linux 3.2 - 3.8	May 2018 – May 2013
xxx.xxx.16.104		Linux 3.10	Nov 2017
xxx.xxx.18.242	VPN	Linux 3.10	Nov 2017
xxx.xxx.18.244	VPN	Linux 3.10	Nov 2017
xxx.xxx.16.245	Netgear GS752TPS Switch	Linux 2.6.8 - 2.6.30	Dec 2004 – Oct 2009
xxx.xxx.16.246	Netgear GS752TPS Switch	Linux 2.6.8 - 2.6.30	Dec 2004 – Oct 2009

xxx.xxx.16.247	Netgear GS752TPS Switch	Linux 2.6.8 - 2.6.30	Dec 2004 – Oct 2009
xxx.xxx.16.248	Netgear GS748T Switch	Linux 2.6.32 - 3.13	Mar 2016 –Apr 2014
xxx.xxx.16.249	Netgear GS748T Switch	Linux 2.6.32 - 3.13	Mar 2016 –Apr 2014
xxx.xxx.16.250	Netgear GS724T Switch	Linux 2.6.32 - 3.13	Mar 2016 –Apr 2014
xxx.xxx.16.251	Netgear GS724T Switch	Linux 2.6.32 - 3.13	Mar 2016 –Apr 2014
xxx.xxx.16.252	Netgear GS748T Switch	Linux 2.6.32 - 3.13	Mar 2016 –Apr 2014
xxx.xxx.16.253	Netgear GS724T Switch	Linux 2.6.32 - 3.13	Mar 2016 –Apr 2014
xxx.xxx.18.254	Router	Linux 3.10	Nov 2017
xxx.xxx.19.244	Cyberoam Router/Firewall	Linux 2.6	Dec 2004
xxx.xxx.90.253	Linksys WRT45G	Linux 3.10	Nov 2017

External Vulnerability Assessment

External Vulnerability Summary

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

Service and port enumeration are the first stage in the external vulnerability assessment to map out the ports which are listening on the given IP addresses and the associated services running on those ports. There were 3 external IP's which were in scope and are shown below along with their host names (28).

Table 28: External IP address

IP Address	Hostname
xxx.xxx.xxx.220	Rds.XXX.co.uk
xxx.xxx.xxx.221	Vpn.XXX.co.uk
xxx.xxx.xxx.222	Rds.XXX.co.uk

During the assessment of the external IP addresses, it was identified that all requests by the probes to 65535 ports were not responded to. Advance scans were conducted to evaluate and bypass the firewall. This produced the results of an SQL server (rsqlserver) running on port 4430 and Microsoft SQL Monitor service on port 1434 at the IP address xxx.xxx.xxx.222.

Enumeration of these ports were conducted and resulted in no further actionable results.

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 fully funded 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.

There's more to the Cyber Resilience Centres...

There are many additional ways to engage with your Regional CRC. If you haven't already, you can join the 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** - CRCs run regular webinars and events on a range of topics relevant to your small business or third sector organisation.

- **Funded solutions** – CRCs offer a range of services like this one, which are designed to address the most pertinent risks affecting SMEs, as identified by policing and Government.

- **Cyber Essentials Certification** - If you are planning to achieve Cyber Essentials or Cyber Essentials Plus certification, your Regional CRC can refer you to IASME who have a list of local suppliers in your region that provide this.

Find your Regional Cyber Resilience Centre here.

Get in touch with us at engagement@cyberpath.co.uk if there's anything else we can help you with.