Monthly report - [Fantastic Five]

1. Executive Summary - Key points and trends of the month

This report presents the findings from our recent cybersecurity monitoring, focusing on newly identified vulnerabilities (CVEs) across several critical systems, including Nessus, Microsoft Windows Server, Linux and Azure, as well as applications like Google Chrome and Microsoft Teams.

Key vulnerabilities identified include a race condition in Nessus that could lead to unauthorised code execution and an SQL injection issue in Azure's MOVEit Transfer application, which could expose sensitive database information. High-severity vulnerabilities in Google Chrome, such as the potential for full system control via heap corruption, highlight the increasing risks from web-based attacks.

For each CVE identified, we have categorised its potential impact and provided recommendations for addressing these risks. The most urgent vulnerabilities—those rated critical or high—should be patched within 10-30 days. These include CVEs in Nessus, Linux, and Azure that could lead to data breaches or service disruptions if left unpatched.

Our recommended mitigation actions focus on keeping systems regularly updated, applying the latest security patches and monitoring emerging threats. In particular, the CVEs affecting critical infrastructure, such as Microsoft Windows Server, must be prioritised to prevent potential denial-of-service attacks or privilege escalations.

To maintain a strong security posture, it is essential to follow a proactive approach that includes regularly reviewing trusted sources like the National Cyber Security Centre (NCSC) and industry blogs to stay informed about new vulnerabilities. Additionally, conducting regular penetration tests will help identify and mitigate risks before they can be exploited.

By following the outlined action plan, including timely patching and continuous monitoring, we aim to significantly reduce the organisation's exposure to cyber risks and ensure the ongoing security of our systems.

Table of Contents

2. Performance Indicators....3

3. Newly Identified CVEs....5

Nessus....5

Linux....5

Azure....6

Azure SQL....6

Microsoft Windows Server....6

Google Chrome....7

Other Software....7

4. Risk Analysis....8

Microsoft Windows Server:....8

Nessus:....8

Linux:....8

Azure:....8

Microsoft Teams:....8

Google Chrome:....8

Other Software:....8

7. Action Plan....12

Nessus....12

Linux....12

Azure....12

Microsoft Windows Server....13

Google Chrome....13

Other Software....13

8. Recommendations....14

1. Regular Software Updates....14

2. Monitoring Emerging Threats....14

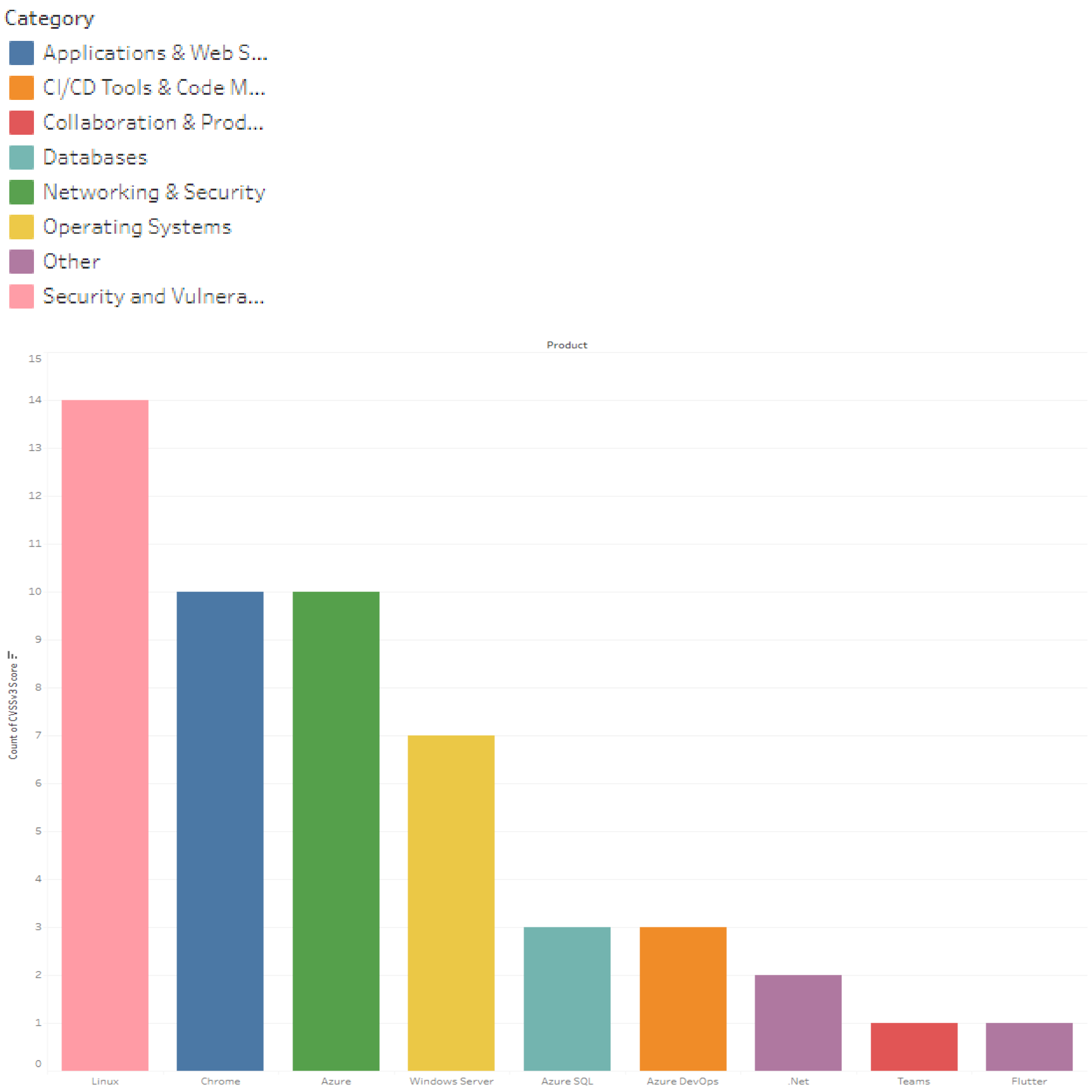
3. Utilising Trusted Resources....14

Conclusion....15

2. Performance Indicators

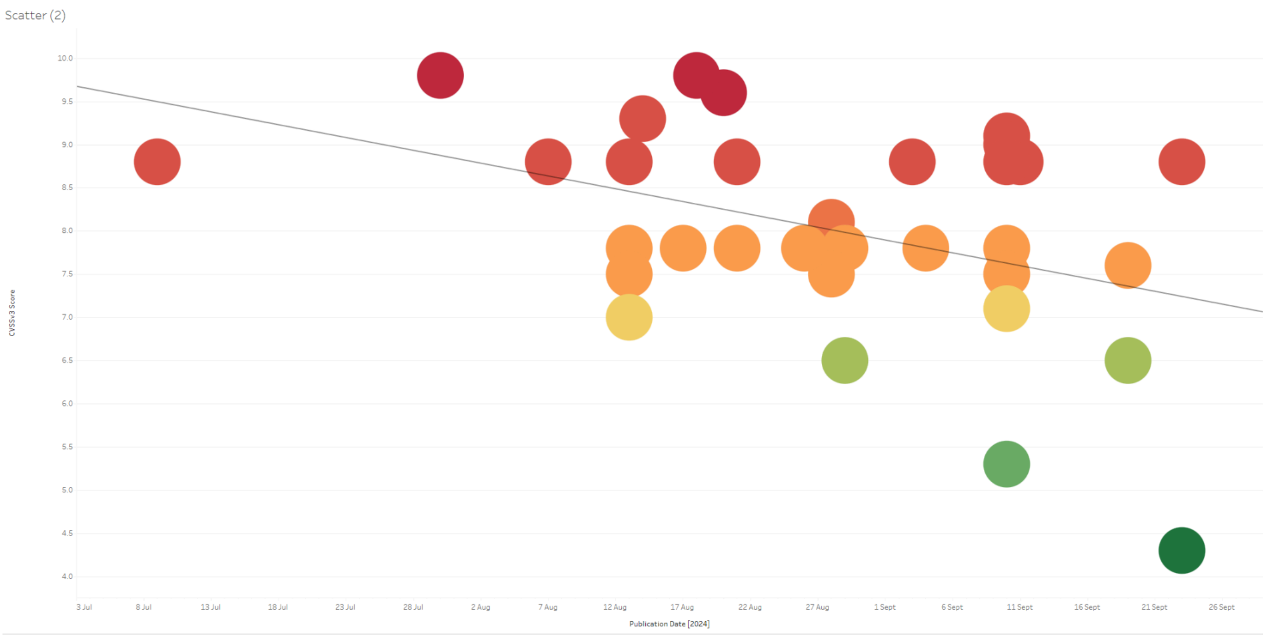
Trend graphs of key metrics over the past three months.

The bar chart below shows the count of vulnerabilities grouped by products and coloured by category.

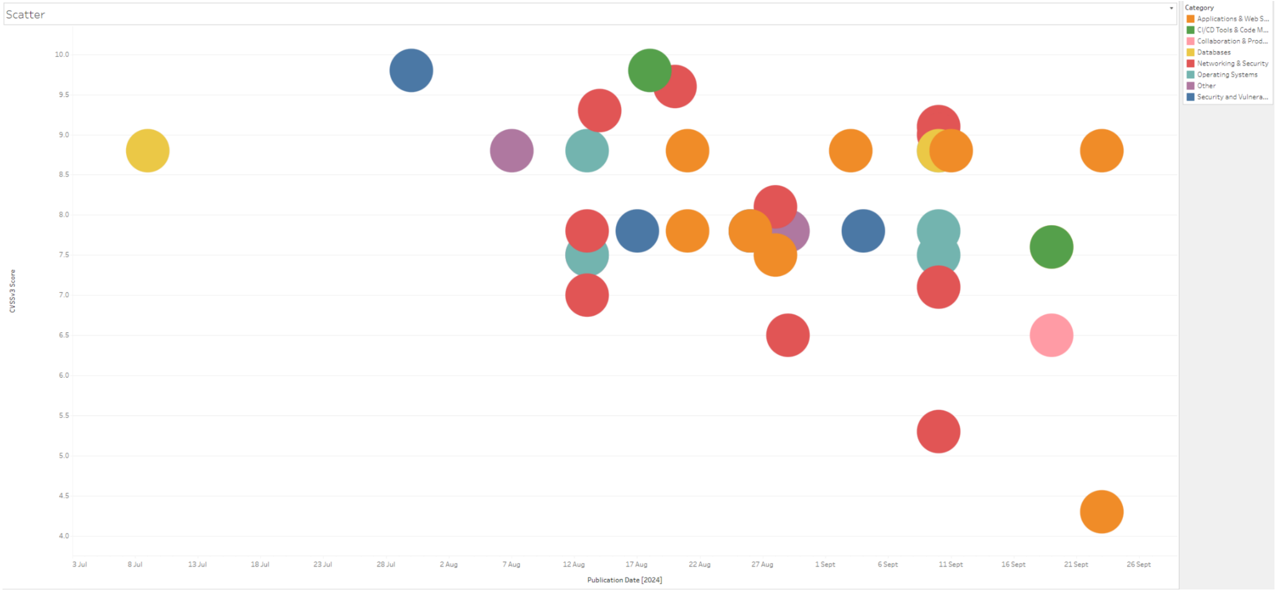


- Linux has the highest number of vulnerabilities, closely followed by Chrome and Azure. These three areas require the most attention, as they represent the most exposed systems in the organisation.
- Other products like Windows Server, Azure SQL and DevOps are also notable, though with fewer vulnerabilities.
- Prioritisation of patching and remediation should focus on Linux, Chrome and Azure first then followed by other critical infrastructure.

The scatter plot below shows the number of vulnerabilities found across all products over the past three months. The scatter plot includes linear regression to display the line of best fit and represent the overall trend.

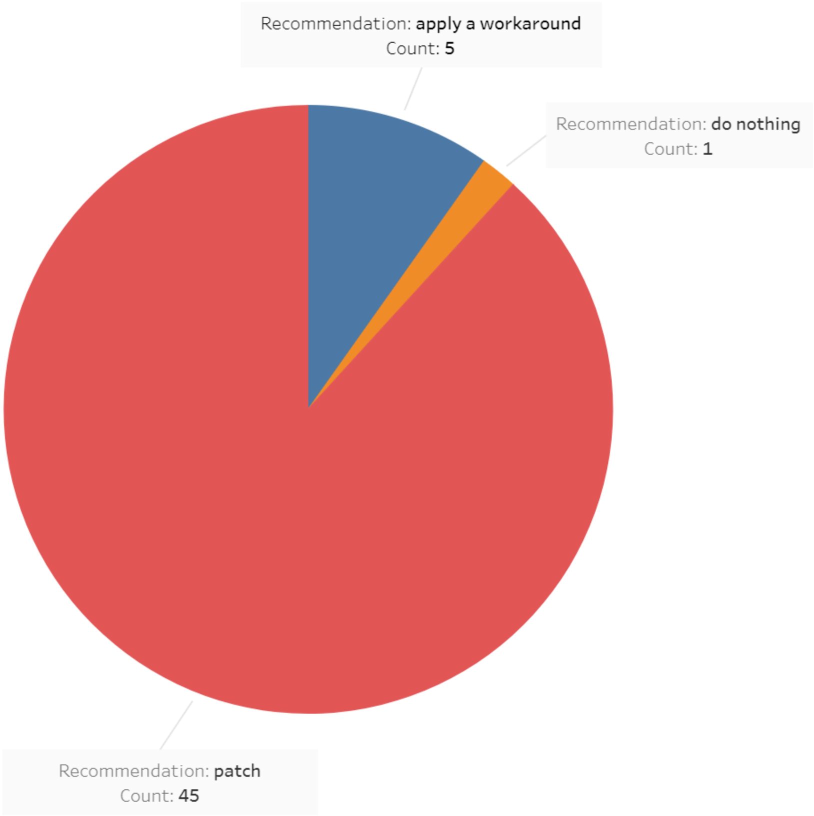


A scatter plot distribution of product CVE's by Category helps provide a clear understanding of the collected data to know which technology products have contained the most vulnerabilities. In the category-based graph, multiple categories are affected, with vulnerabilities spanning across various products and systems.



The high concentration of critical vulnerabilities (with CVSS scores above 8.0) occurs primarily in the months of July and August. This indicates a period where critical vulnerabilities were more frequently disclosed, requiring immediate attention.

The pie chart shows the distribution of recommended action types. Knowing which recommendation is best suited for each technology product provides effective risk management and security posture.



- As clearly shown in the pie chart, the ‘patch’ is the most recommended action when resolving all the system vulnerabilities.
- A small portion requires workarounds (5 instances) where no patch is available yet, and just one instance recommends no action.

Patch management will be our main priority since most vulnerabilities have patches available. However, we will monitor cases where workarounds are applied to ensure that they are addressed with future patches.

3. Newly Identified CVEs

The table below presents a list of newly identified Common Vulnerabilities and Exposures (CVEs). For the purpose of this report, we have selected three CVEs from each software provided, focusing on those most relevant. Additional information on other CVEs, which we have compiled over a few months is available in a separate spreadsheet.

Additional Information:

- **Nessus:**
  In the vulnerability management category, Kali Linux was initially highlighted for monitoring. However, as Kali Linux serves as the operating system for installing Tenable Nessus, we have decided to include both Kali Linux and Nessus in our monitoring process. For Kali Linux we have looked at vulnerabilities in the Linux kernel.
- **Other Software:**
  The table also includes other software, such as .NET and Microsoft Teams.

Nessus		
CVE	CVE Description	Potential impact description
CVE-2024-3290	A race condition vulnerability exists where an authenticated, local attacker on a Windows Nessus host could modify installation parameters at installation time, which could lead to the execution of arbitrary code on the Nessus host.	If Nessus were to be installed on a Windows environment and a local attacker had gained access into the system such that he's able to modify installation parameters, arbitrary code execution could lead to data leakage, password theft, ransomware attacks and other threats.
CVE-2024-3289	When installing Nessus to a directory outside of the default location on a Windows host, Nessus versions prior to 10.7.3 did not enforce secure permissions for sub-directories. This could allow for local privilege escalation if users had not secured the directories in the non-default installation location.	If an outdated version of Nessus is installed on Windows and the cited pre-condition is true, this could lead to data leakage.
Linux		
CVE	CVE Description	Potential impact description
CVE-2024-42154	TCP_METRICS_ATTR_SADDR_IPV4 field isn't validated to be at least 4 bytes long	Anything could be in the mentioned data field in an incoming packet since there is no validation on the length of the field. This could lead to data leakage, password theft, ransomware attacks and other threats.

CVE-2024-43858	An array of out-of-bounds vulnerabilities in the DiFree function in the Linux kernel	This could used to gain access to sensitive data in memory and lead to data leakage.
CVE-2024-44934	A use-after-free vulnerability was found in the Linux kernel's network bridge multicast functionality. The issue occurs when a port is removed while garbage collection cycles are still running, potentially leading to system crashes or further exploits.	This could lead to downtime due to the system crashing.
Azure		
CVE	CVE Description	Potential impact description
CVE-2023-34362	SQL injection vulnerability has been found in the MOVEit Transfer web application.	This could allow an unauthenticated attacker to gain access to MOVEit Transfer's database.
CVE-2024-38108	Azure Stack Hub Spoofing Vulnerability. A user (victim) logged on to a virtual machine would need to be tricked.	Attackers could enable the user to explicitly download and execute malicious code in their web browser.
CVE-2024-38109	An authenticated attacker can exploit a Server-Side Request Forgery (SSRF) vulnerability in Microsoft Azure Health Bot to elevate privileges over a network.	If successful, an attacker has the potential to access all areas of the system by elevating their privileges, this could lead to customer and individual data being stolen/leaked.
Azure SQL		
CVE	CVE Description	Potential impact description
CVE-2024-28928	Remote code execution vulnerability enabled by tricking an authenticated user into attempting to connect to a malicious SQL server database via a connection driver.	This could result in the database returning malicious data that could cause arbitrary code execution on the client.
CVE-2024-37980	The product does not properly assign, modify, track, or check privileges for an actor, creating an unintended sphere of control for that actor.	Attackers can elevate their privileges and gain access to information that is more private/personal data such as financial and ipp.
CVE-2024-43474	An attacker who successfully exploited this vulnerability could potentially read small portions of heap memory.	Potential for an attacker to disclose information.
Microsoft Windows Server		
CVE	CVE Description	Potential impact description
CVE-2024-43455	Windows Remote Desktop Licensing Service Spoofing Vulnerability.	This could lead attackers to trick the user into accessing user credentials which the attackers could use to gain higher authentication resulting in more serious damage to business services.

CVE-2024-38014	The Windows Installer Elevation of Privilege Vulnerability lets attackers use Windows installer elevation to gain higher privileges than intended.	This vulnerability could lead to data breaches through code executions. It is important to apply the least privilege principle as a way for users to be granted the minimum level of access or permissions necessary to perform its intended function reducing the risk of malicious use.
CVE-2024-38247	Windows Graphics Component Elevation of Privilege Vulnerability.	This could lead to the system crashing and service disruptions. Attackers may gain privileges, allowing them to access sensitive files and system configurations.

Google Chrome

CVE	CVE Description	Potential impact description
CVE-2024-7973	A remote attack to perform an out-of-bound memory read by exploiting a crafted PDF file.	This vulnerability could lead to arbitrary code execution or other exploits, allowing attackers to gain access to sensitive parts of memory.
CVE-2024-8194	The vulnerability affected V8 Google Chrome's JavaScript engine in Chrome, allowing a remote attacker to exploit heap corruption by crafting a malicious HTML page.	Attackers could potentially take full control of the affected system, gaining access to sensitive data, modifying files or performing additional attacks.
CVE-2024-7979	Insufficient data validation in the installer for Google Chrome on Windows allows local attackers to escalate privileges via crafted symbolic links.	This vulnerability could enable a local attacker to gain elevated privileges, compromising system security by allowing unauthorised access to sensitive data or critical system functions.

Other Software

CVE	CVE Description	Potential impact description
CVE-2024-38168	.Net. in ASP.NET HTTP.sys web server. This is a Windows OS only vulnerability.	Attackers through unauthenticated requests may trigger a Denial of Service attack.
CVE-2024-45302	Potential for CRLF injection into HTTP headers when using HTTP/1.1. This can lead to the injection of additional HTTP headers or the smuggling of whole HTTP requests.	Can escalate to request splitting, potentially enabling Server Side Request Forgery (SSRF) attacks.
CVE-2024-38197	The attacker is only able to modify the sender's name of the Teams message.	This vulnerability could allow for an attacker to impersonate others leading to possible man in the middle attacks.

4. Risk Analysis

This section addresses the potential risks posed by identified CVE's, the prioritisation and urgency in addressing each issue.

Microsoft Windows Server:

The Microsoft Windows Server is vulnerable to enabling attackers to run arbitrary code on the server which causes the service to become unavailable to authorised users within the business. This kind of attack is known as a denial of service attack. Understanding the significance of the Windows Server operating system when it comes to networked resources, applications and services makes it crucial to patch the vulnerabilities to be able to protect sensitive data.

Nessus:

It is possible that vulnerable versions of Nessus are installed on company devices, hence there is a risk of data leakage, password theft, ransomware attacks and other threats.

Linux:

It is possible that company devices running Linux are not updated regularly, hence there is a risk of data leakage, password theft, ransomware attacks and other threats.

Azure:

Cloud services are vulnerable to remote code execution and spoofing attacks. More so when users are tricked into executing malicious actions. This could result in unauthorised data access and disruptions.

Microsoft Teams:

Given that Microsoft Teams is crucial for internal collaboration, ensuring that such vulnerabilities are patched is essential to maintaining the security of communication and data within the organisation.

Google Chrome:

These vulnerabilities highlight the importance of timely patching and mitigation, especially focusing on the remote exploitation vectors which could have wide-reaching impacts on system security, business continuity, and data protection.

Other Software:

Each vulnerability is evaluated based on its CVSS Score, Likelihood, and Severity according to the Risk Management Scales. The goal is to identify and prioritise risks that pose the greatest threat to the organisation, considering both their technical impact and the potential consequences on business operations.

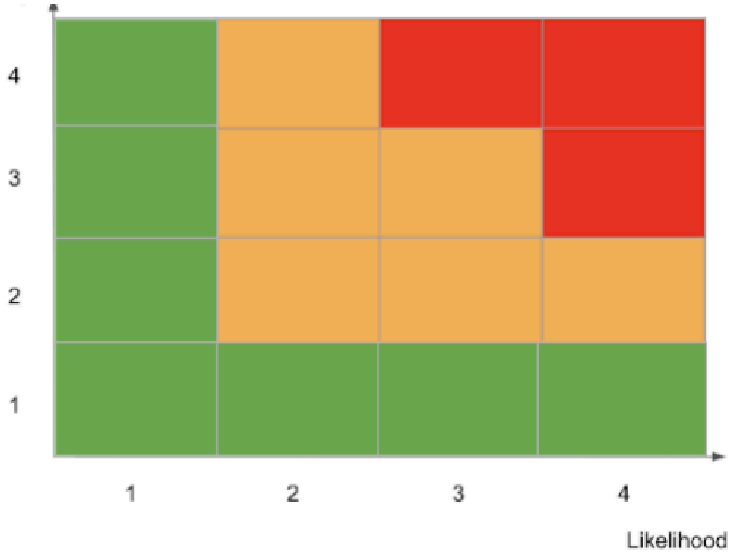
The following table highlights the **Product**, **CVE**, **CVSS Score**, **Likelihood × Severity** *(see risk matrix below)*, and a brief **Business Context** to explain why each vulnerability is significant and how it could impact operations:

This does not include all CVEs found during the weekly report, but those deemed worthy of inclusion based on their relevance to the business.

Product	**CVE**	**CVSS Score**	**'Likelihood X Severity' Score**	**Business Context**
Linux	CVE-2024-42154	9.8 (Critical)	Frequent, Critical (12)	High risk due to the critical nature of unvalidated fields leading to potential data leakage.
Azure	CVE-2023-34362	9.8 (Critical)	Frequent, Critical (12)	SQL injection vulnerability with a high likelihood due to web exposure, leading to critical risks.
Nessus	CVE-2024-3290	8.8 (High)	Frequent, Serious (9)	High likelihood of exploitation due to access potential and impact on data security.
Google Chrome	CVE-2024-7973	8.8 (High)	Frequent, Serious (9)	Frequent exploitation risk due to common browser usage, leading to remote code execution.
Google Chrome	CVE-2024-8194	8.8 (High)	Frequent, Serious (9)	High likelihood of being targeted due to its potential for full control over affected systems.
Google Chrome	CVE-2024-7979	7.8 (High)	Frequent, Serious (9)	Elevated risk due to local attackers exploiting privilege escalation vulnerabilities, compromising system integrity and confidentiality on widely used Windows platforms.
Nessus	CVE-2024-3289	8.5 (High)	Conceivable, Serious (6)	Moderate likelihood with significant impact if exploited, leading to privilege escalation.
Linux	CVE-2024-43858	8.0 (High)	Conceivable, Serious (6)	Likelihood of exploitation is conceivable, with serious impact on

				data security.
Azure	CVE-2024-38108	9.3 (Critical)	Conceivable, Serious (6)	Risk of spoofing with moderate likelihood, significant due to its potential to mislead users.
Microsoft Windows Server	CVE-2024-43455	8.8 (High)	Conceivable, Serious (6)	Spoofing vulnerability that can lead to credential theft, a moderate likelihood of occurrence.
Microsoft Windows Server	CVE-2024-38014	7.8 (High)	Conceivable, Serious (6)	Risk of privilege escalation with serious potential impact on system security.
Other Software (.Net)	CVE-2024-45302	7.2 (High)	Conceivable, Serious (6)	Potential for SSRF attacks, making it a significant risk if exploited, though less frequently targeted.
Microsoft Windows Server	CVE-2024-38247	7.8 (High)	Conceivable, Significant (4)	Vulnerability may cause service disruptions, but it has a lower likelihood of direct exploitation.
Linux	CVE-2024-44934	7.5 (High)	Conceivable, Significant (4)	Moderate impact, affecting system stability but less likely to be targeted frequently.
Microsoft Teams	CVE-2024-38197	6.5 (Medium)	Conceivable, Significant (4)	Moderate risk due to potential unauthorised access, but less likely to be a frequent target.
Other Software (.NET)	CVE-2024-38168	6.0 (Medium)	Conceivable, Significant (4)	Denial of service vulnerability that is conceivable but with limited overall impact.

Risk Matrix



Risk Scenarios Likelihood

Level	Definition
1 - Improbable	The event has never occurred and is unlikely to happen in the coming months. It’s an exceptional situation.
2 - Conceivable	The event has occurred in the last three years or could happen in the coming months.
3 - Frequent	The event has occurred in the last year or could happen in the coming year.
4 - Very frequent	The event has occurred regularly in the last year or will certainly happen several times in the coming months.

Risk Scenarios Severity

Level	Definition
1 - Minor	Negligible consequences for the organisation: no impact on operations of the activity.
2 - Significant	Significant but limited consequences for the organisation: degradation in the performance of the activity.
3 - Serious	Substantial consequences for the organisation: high degradation in the performance of the activity.
4 - Critical	Disastrous consequences for the organisation: incapacity to ensure all or a portion of its activity.

7. Action Plan

This section outlines the Action Plan for mitigating vulnerabilities identified in the CVEs. It details the security measures, the responsible parties, and the associated timeframes. The timeline provided below is practices from other organisations and serves as a guide for our own process. It is structured to ensure vulnerabilities are addressed efficiently without overwhelming the responsible teams, particularly when managing multiple issues simultaneously. It is important to ensure that all vulnerabilities in your technology are patched to prevent bad actors from exploiting them. Therefore, we propose the following remediation and security measures to protect your security and ensure that services continue to operate normally.

Severity	**Timeline**
Critical *(CVSS 9 - 10)*	10 days
High *(CVSS 7 - 8.9)*	30 days
Medium *(CVSS 5 - 6.9)*	60 days
Low *(CVSS less than 4.9)*	90 days

<table>
<tr><th colspan="4"><b>Nessus</b></th></tr>
<tr><td>CVE</td><td>Security measure</td><td>Responsible parties</td><td>Timeframe</td></tr>
<tr><td>CVE-2024-3290</td><td>Ensure no vulnerable versions of Nessus are installed on company devices.</td><td>Cyber security team.</td><td>30 days.</td></tr>
<tr><td>CVE-2024-3289</td><td>Ensure no vulnerable versions of Nessus are installed on company devices.</td><td>Cyber security team.</td><td>30 days.</td></tr>
<tr><th colspan="4"><b>Linux</b></th></tr>
<tr><td>CVE</td><td>Security measure</td><td>Responsible parties</td><td>Timeframe</td></tr>
<tr><td>CVE-2024-42154</td><td>Ensure all devices running linux are updated.</td><td>System administrators.</td><td>10 days.</td></tr>
<tr><td>CVE-2024-43858</td><td>Ensure all devices running linux are updated.</td><td>System administrators.</td><td>30 days.</td></tr>
<tr><td>CVE-2024-44934</td><td>Ensure all devices running linux are updated.</td><td>System administrators.</td><td>30 days.</td></tr>
<tr><th colspan="4"><b>Azure</b></th></tr>
<tr><td>CVE</td><td>Security measure</td><td>Responsible parties</td><td>Timeframe</td></tr>
<tr><td>CVE-2023-34362</td><td>Apply the recommended patch</td><td>IT Team</td><td>10 days.</td></tr>
<tr><td>CVE-2024-38108</td><td>Apply the recommended patch</td><td>IT Team</td><td>10 days.</td></tr>
</table>

CVE-2024-38109	Apply the recommended patch	IT Team	10 days
CVE-2024-28928	Apply the recommended patch	IT Team	30 days
CVE-2024-37980	Apply the recommended patch	IT Team	30 days
CVE-2024-43474	Apply the recommended patch	IT Team	30 days
Microsoft Windows Server			
CVE	Security measure	Responsible parties	Timeframe
CVE-2024-43455	Ensure that the system is fully updated to Microsoft's latest security patches. Configure firewalls to restrict access to Remote Desktop services only from trusted networks or IP addresses.	IT team.	30 days.
CVE-2024-38014	Ensure that Microsoft applies the latest security updates.	System administrators.	30 days.
CVE-2024-38247	Ensure to update to the latest patches and that they are appropriate to the system.	System administrators.	30 days.
Google Chrome			
CVE	Security measure	Responsible parties	Timeframe
CVE-2024-7973	Ensure timely patching of the affected PDF viewing software and implement updates across all systems.	System administrators.	30 days.
CVE-2024-8194	Apply security updates to Google Chrome and the V8 JavaScript engine immediately upon release.	System administrators.	30 days.
CVE-2024-7979	Update to the latest version of Google Chrome to fix the data validation issue in the installer.	System administrators.	30 days.
Other Software			
CVE	Security measure	Responsible parties	Timeframe
CVE-2024-38168	Update .NET to version 8.0.8 or later to prevent denial-of-service attacks.	System administrators.	60 days.
CVE-2024-45302	Apply the latest security patches to mitigate this vulnerabilitity.	IT Management.	30 days.
CVE-2024-38197	Ensure the latest software updates are applied to prevent exploitation.	IT Management.	60 days.

8. Recommendations

The overarching aim of our recommendations is to prevent vulnerabilities from arising and adopt a proactive approach, rather than reacting once issues have already occurred. From our Action Plan, a key focus is on ensuring that software and systems remain up to date. But what specific actions can we take to achieve this?

1. Regular Software Updates

Maintaining up-to-date software is crucial. This includes not only application software but also firewalls on servers and operating systems across all devices, such as computers and laptops. Regular updates help address known vulnerabilities and improve overall system security.

2. Monitoring Emerging Threats

It is essential to stay informed about potential exploits or vulnerabilities related to the software in use. Regularly checking for updates on security threats ensures that any emerging risks are identified and addressed promptly.

3. Utilising Trusted Resources

Many trusted sources, such as software vendors and government agencies, provide valuable information, advice, and statistical insights that can help you remain proactive in your security efforts. Making use of these resources effectively allows you to stay ahead of potential threats and reduce the likelihood of vulnerabilities appearing in your systems.

Below are some recommended resources that should be monitored periodically:

- UK Government Cyber Security Breaches Survey
- National Cyber Security Centre (NCSC) Blog
- Microsoft Security Blog
- Tenable Security Blog
- Linux Security Blog
- CVE Details Database

By following these actions and making use of the information provided by trusted sources, you can significantly enhance your monitoring and remediation processes, ensuring a more secure and resilient environment.

Conclusion

In conclusion, as technology is frequently updated that means it is possible that new vulnerabilities may appear. Hence, it is important to apply penetration testing as a way to help identify vulnerabilities and then patch them to continue protecting sensitive information and to make sure the technology used is protected from bad actors.