IJYI

CYBER SECURITY Watch

By Samuel, Greg, Darius, Ray, James

United we secure, together we excel

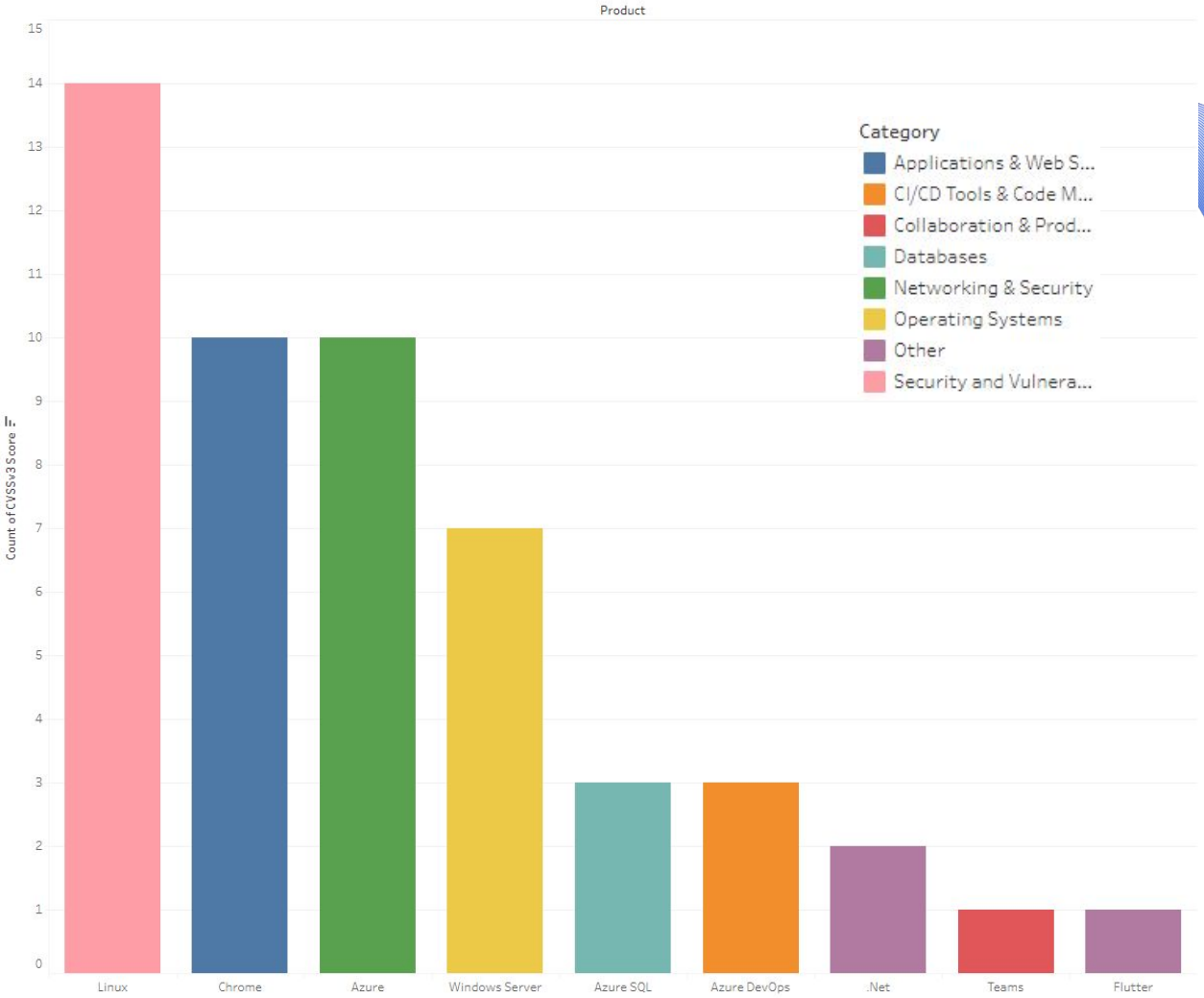
IJYI

Objective of this report

Today we will be sharing the findings from the cyber security watch performed by the Fantastic 6, this report focuses on the following assets

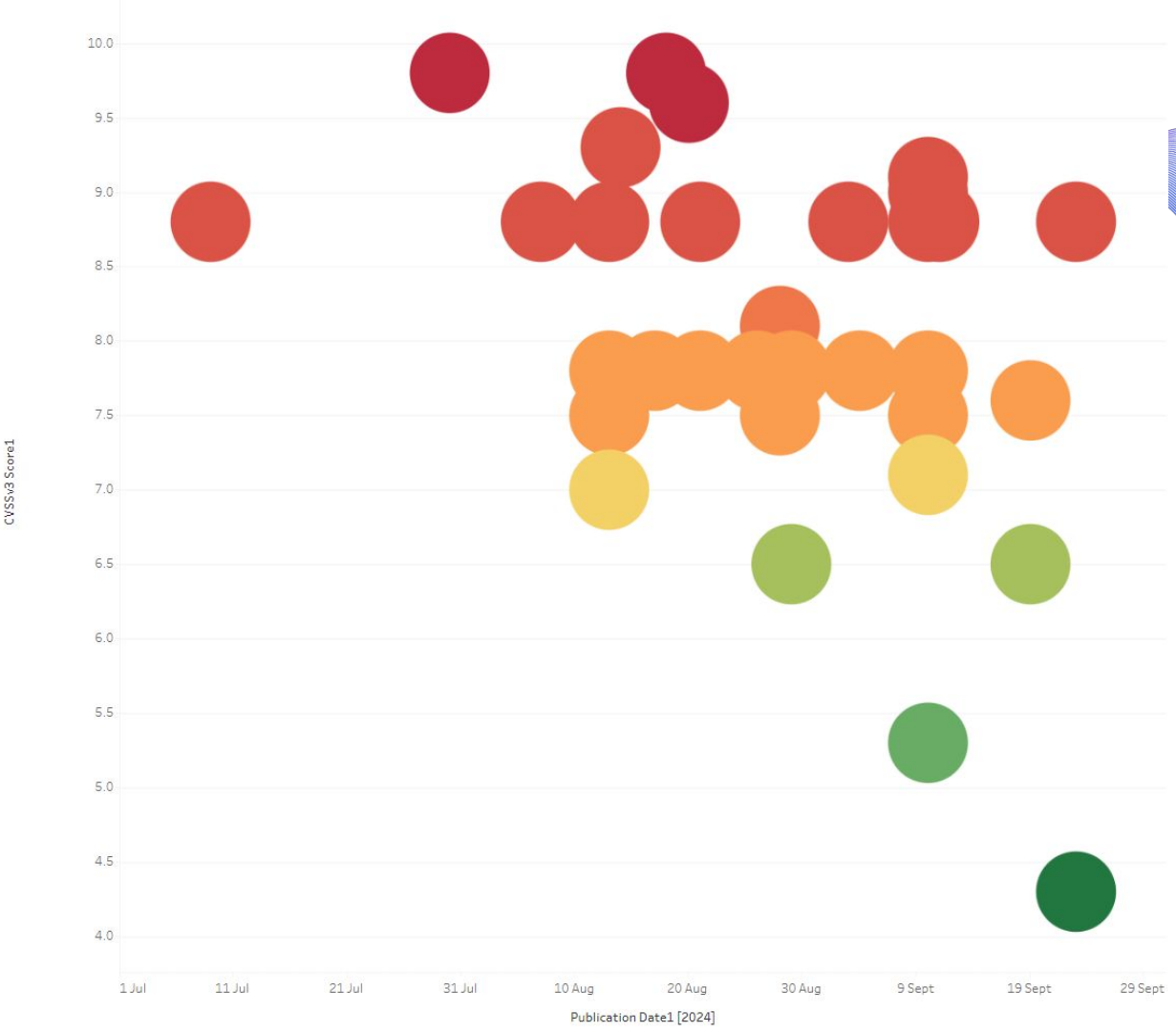
- Google Chrome
- Azure
- Microsoft Windows Server
- Linux
- Nessus

By Product


Product
Count of CVSSv3 Score
15
14
13
12
11
10
9
8
7
6
5
4
3
2
1
0
Linux
Chrome
Azure
Windows Server
Azure SQL
Azure DevOps
.Net
Teams
Flutter
Category
Applications & Web S...
CI/CD Tools & Code M...
Collaboration & Prod...
Databases
Networking & Security
Operating Systems
Other
Security and Vulnera...

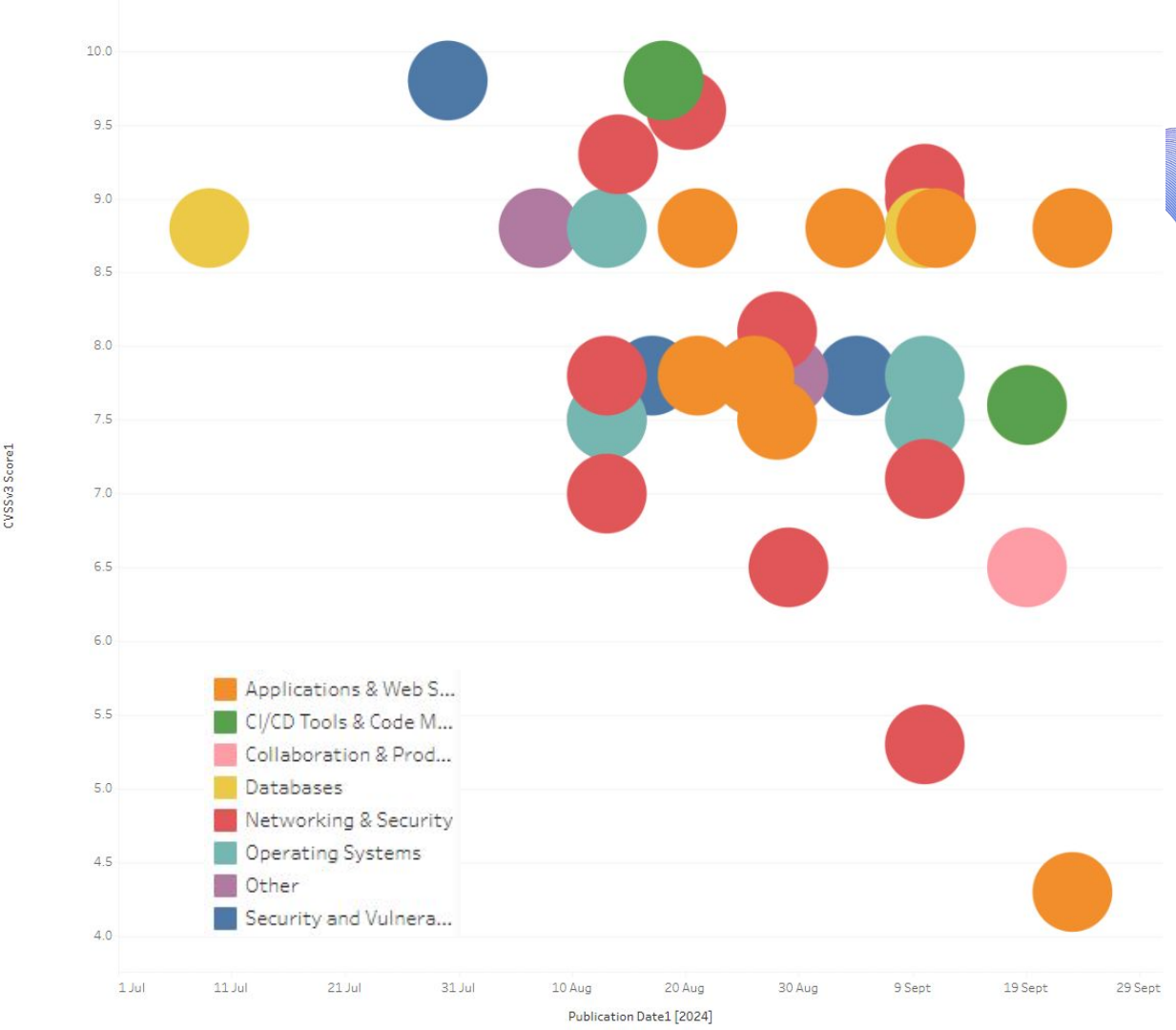
IJYI

All CVEs



IJYI

By Category



IJYI

Critical CVEs

Google Chrome - CVE-2024-7973
Remote Code Execution via Crafted PDF

- **CVSS Score**: 8.8
- **Impact**: Attacker can exploit an out-of-bound memory read by crafting a malicious PDF, can lead to arbitrary code execution on the affected system.
- **Relevance**: Chrome is widely used. employees may unknowingly open malicious PDFs that could compromise their workstations. This can lead to malware infections or data theft.
- **Recommendation**: Ensure all instances of Google Chrome are updated to the latest version and implement controls to prevent the opening of untrusted PDFs.

IJYI

Critical CVEs

Windows Server - CVE-2024-43455
Remote Desktop Licensing Spoofing

- **CVSS Score**: 8.8
- **Impact**: Allow attackers to trick users into giving away credentials via the Remote Desktop Licensing Service.
- **Relevance**: Exploitation of remote desktop services could allow attackers to access critical systems, potentially leading to widespread disruptions and data loss.
- **Recommendation**: Apply the latest security updates to Windows Server.

IJYI

Critical CVEs

Azure - CVE-2024-38220
Elevation of Privilege

- **CVSS Score**: 9
- **Impact**: This vulnerability in Azure Stack Hub allows privilege escalation which can be exploited remotely.
- **Relevance**: This vulnerability could grant hackers unauthorised admin access, leading to data breaches and or service disruption.
- **Recommendation**: Immediate patching of Azure with the latest security updates.

IJYI

Critical CVEs

Linux (Kali) - CVE-2024-42154
Buffer overflow

- **CVSS Score**: 9.8
- **Impact**: This vulnerability involves a missing field length validation in the Linux kernel, which could result in serious data leakage or potential compromise of the system's security.
- **Relevance**: Linux is often critical for backend operations . Vulnerability could lead to unauthorized access and data theft.
- **Recommendation**: Immediate patching of the Linux kernel with the latest security updates.

Critical CVEs

Nessus - CVE-2024-3290
Race condition

- **CVSS Score**: 8.2
- **Impact**: 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.
- **Relevance**: Arbitrary code execution could lead to data leakage, password theft, ransomware attacks and other threats.
- **Recommendation**: Ensure no vulnerable versions of Nessus are installed on company devices.

IJYI

Critical CVEs

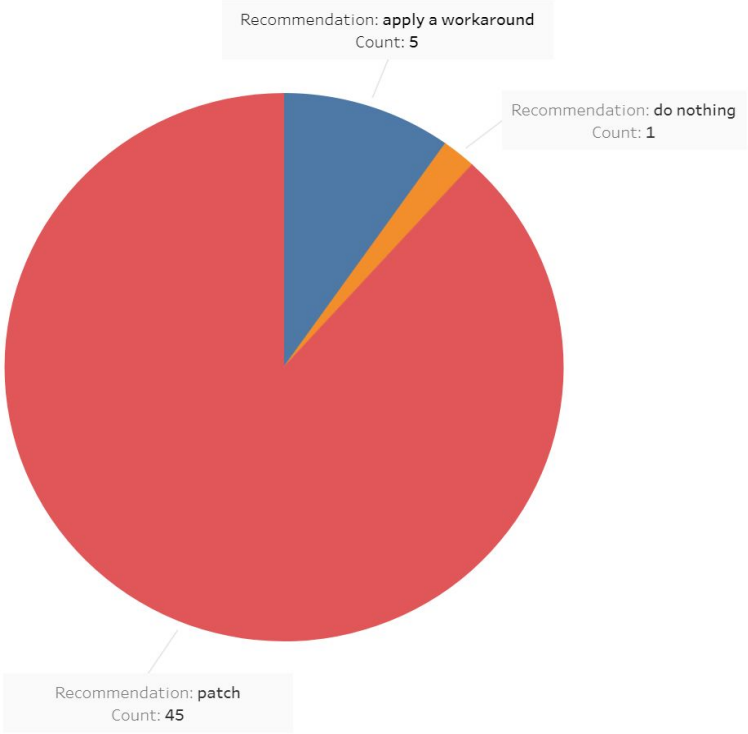
Microsoft Azure DevOps - CVE-2023-34362
SQL injection vulnerability in MOVEit Transfer application.

- **CVSS score**: 9.6
- **Impact:** Could allow an unauthenticated attacker to gain access to MOVEit Transfer's database.
- **Relevance:** An attacker could expose sensitive information stored on the database.
- **Recommendation:** Apply the latest security patch/updates from Microsoft.

IJYI

Impact Type

Recommendations



IJYI

Recommendations

- Regular Software Updates
- Monitoring Emerging Threats
- Utilising Trusted Resources

IJYI

Summary

- **Key systems affected** - Vulnerabilities identified across critical systems, including Nessus, Microsoft Windows Server, Linux, Azure,Google Chrome and Microsoft Teams

- **High risk Cve's** - Urgent Vulnerabilities include Nessus (unauthorised code execution) and Azure MOVEit Transfer (SQL injection). Google Chrome vulnerabilities pose risks of full system control.

IJYI

Summary

- **Critical patching** - High and critical CVEs must be patched within 10-30 days to prevent data breaches and service disruptions.
- **Mitigation strategy** - Regular updates, prompt security patches, and continuous monitoring are essential. Prioritise key systems like Microsoft Windows Server to prevent major attacks.
- **Proactive Security** - Stay informed via trusted sources, conduct regular penetration testing, and follow a proactive approach to minimise cyber risks and safeguard the organisation’s systems.


United we secure, together we excel