

VULNERABILITY REPORT

JULY 2026 - OCTOBER 2026

OUR MISSION IS SIMPLE;

To combine the best possible customer experience, with market leading delivery for every client, every time.

Contact

Phone	+44 (0)1789 608708
Website	www.istormsolutions.co.uk
Email	info@istormsolutions.co.uk

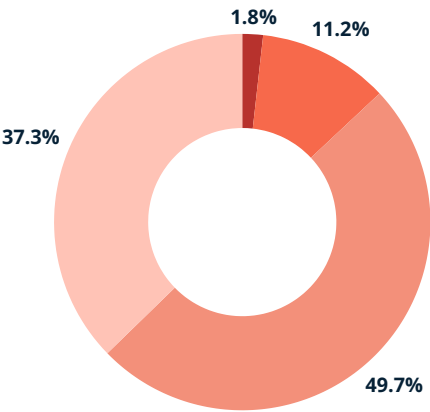
Quarter 3 Vulnerability Report

Summary

From 1st July 2026 to the 30th September 2026, a total of 199 vulnerabilities were identified, categorised by severity as follows:

Severity:

● Critical	3
● High	19
● Medium	84
● Low	63



The identification of 22 High or Critical vulnerabilities highlights the continued importance of regular security testing and timely remediation.

Vulnerabilities by Type

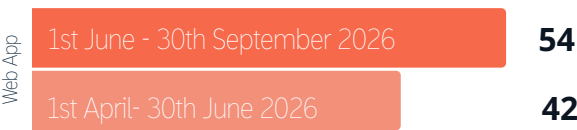
Of these vulnerabilities **54** were associated with Web Applications, **47** were Internal Infrastructure, and **31** were External Infrastructure.

Top Testing Type: Web Application & Internal Infrastructure

Web Application and Internal Infrastructure testing accounted for the highest number of identified vulnerabilities during Q3.

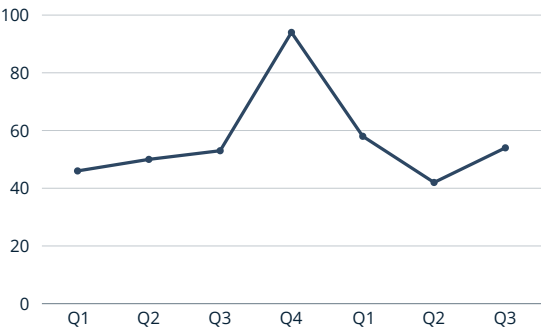
These findings demonstrate that vulnerabilities can exist across both externally accessible applications and internal environments. As organisations continue to expand their digital estates and rely on increasingly interconnected systems, maintaining visibility across both external and internal attack surfaces remains essential.

Regular testing helps organisations identify weaknesses before they can be exploited, while providing a clear basis for prioritising remediation activity based on risk.



54 vulnerabilities: highlighting a continually high trend in Web Application vulnerabilities.

Web App Quarterly Trend



Top Master Vulnerabilities

Of the vulnerabilities identified, the following were the most frequent or high-risk:

- | | |
|---|--------|
| ◦ Web Access Control: Broken access control | High |
| ◦ Azure: Defender for Azure API not enable | High |
| ◦ Web Applications: Inadequate Input Validation | Medium |

These recurring findings highlight several areas requiring continued attention, particularly access control, software lifecycle management and legacy technology. Broken access control can allow users to access functionality or information beyond their intended permissions, potentially resulting in unauthorised access to sensitive data or systems.

Outdated and unsupported software presents an increased security risk as vulnerabilities may remain unpatched and vendors may no longer provide security updates. Similarly, legacy protocols such as SMBv1 are known to introduce significant security weaknesses and should be removed or disabled wherever possible.

Notable Trends

Based on testing performed during Q3 2026, iSTORM observed several recurring themes across client environments:

Access control remains a key area of risk

Broken access control continues to be identified within web applications, reinforcing the importance of robust authentication and authorisation controls. Organisations should regularly review permissions and test applications from the perspective of different user roles.

Legacy and unsupported technologies continue to create exposure

Outdated software and legacy protocols remain a recurring finding. Organisations should maintain accurate asset inventories, establish clear patching processes and have a defined approach for replacing or mitigating unsupported technologies.

Internal environments require the same level of attention as external-facing systems

The number of vulnerabilities identified within internal infrastructure demonstrates that an organisation's security posture cannot be assessed solely from its internet-facing attack surface. Internal systems should be regularly tested to understand what an attacker could achieve following an initial compromise.

Prioritisation is essential

With 199 vulnerabilities identified, remediation should be driven by risk rather than simply the number of findings. Critical and High vulnerabilities should be prioritised, while Medium and Low findings should be managed through an appropriate remediation programme.

Recommendations from our Testers

Based on the findings identified during, iSTORM's testers recommend the following:

Access Control

Regularly review user permissions to help ensure people can only access the information and functions they need.

Azure API Protection

Review the security protections available for your Azure APIs and consider whether additional monitoring would be beneficial.

Input Validation

Review how applications handle user input to help prevent unexpected or potentially harmful data from being processed.

Outdated Software

Keep software up to date and plan for the replacement of products that are no longer supported.

Legacy Protocols

Review older protocols, such as SMBv1, and disable them where they are no longer required.

Internal Security

Regularly assess internal systems to identify weaknesses that may be less visible from outside the organisation.

Remediation Priorities

Address the most significant risks first and maintain a clear plan for resolving remaining findings.

We are the Humans in the Loop

At iSTORM, we believe effective cybersecurity is about more than identifying vulnerabilities. It is about understanding what they mean, assessing the risks they present and helping organisations make informed decisions about what to do next.

Our testers bring technical knowledge, experience and real-world insight to every engagement, helping distinguish genuine risks and providing practical recommendations tailored to each environment.

By combining the efficiency of technology with the judgement of experienced security professionals, iSTORM helps organisations move beyond simply finding vulnerabilities to understanding and reducing their exposure.

Because finding vulnerabilities is only the first step. Understanding them, prioritising them and taking action is what makes the difference.

How Can We Help?



As an award-winning GRC consultancy, our business is really about people. We work with you to understand, your business, and your requirements. Our testing approach is driven by threat intelligence, incorporating insights from global and industry-specific cyber trends to ensure relevancy and accuracy in our assessments.

Threats are evolving rapidly, and staying ahead requires more than just reactive measures. Our team can help you proactively identify, assess, and mitigate risks before they impact your business.

Get in Touch

Whether you're looking to strengthen your web applications, secure your infrastructure, or gain insight into emerging threats, we're here to help.

For more information about how iSTORM can support your organisation, contact us today.

Contact

Phone	+44 (0)1789 608708
Website	www.istormsolutions.co.uk
Email	info@istormsolutions.co.uk