

VULNERABILITY REPORT

APRIL 2026 - JUNE 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

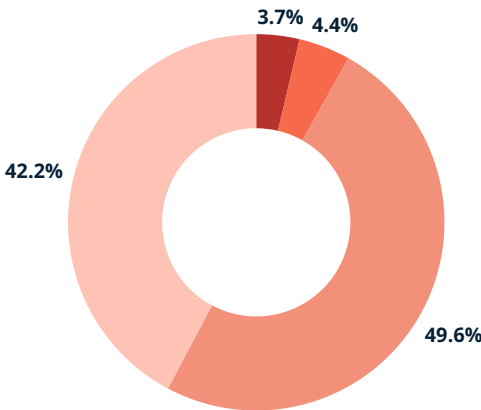
Quarter 2 Vulnerability Report

Summary

From 1st April 2026 to the 30th June 2026, a total of 155 vulnerabilities were identified, categorised by severity as follows:

Severity:

● Critical	5
● High	6
● Medium	67
● Low	57

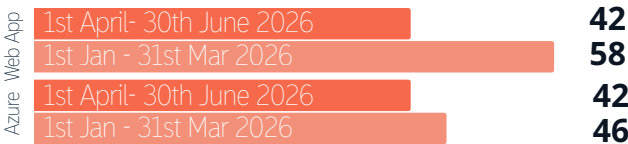


Vulnerabilities by Type

Of these vulnerabilities 42 were associated with Web Applications, 42 were Azure, and 20 were Internal Infrastructure.

Top Testing Type: Web Application & Azure

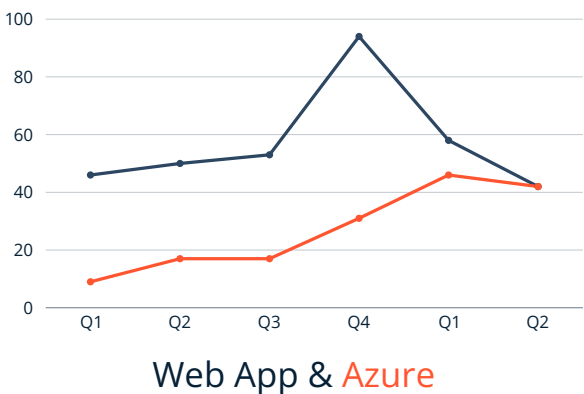
Between 1 April 2026 and 30 June 2026, iSTORM identified a total of 155 vulnerabilities. Web Application and Azure-related vulnerabilities were the most frequently identified categories, with **42** findings recorded in each.



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

These findings highlights that app security remains a significant area of risk for many organisations. Common findings continue to stem from insecure coding practices, insufficient input validation, authentication weaknesses, and outdated software components. Similarly, the 42 Azure-related vulnerabilities demonstrate that cloud security and identity management remain key challenges.

Quarterly Vulnerability 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 common security challenges experienced across organisations, particularly in relation to vulnerability management, identity and access governance, and secure software maintenance.

Notable Trends & Recommendations

Based on testing performed during Q2 2026, iSTORM observed several recurring themes across client environments:

Outdated software continues to be one of the most common High severity findings, reinforcing the importance of effective patch management processes.

Identity and access management weaknesses, particularly within **cloud environments**, continue to be a recurring theme. Strengthening governance, conducting regular access reviews, and enforcing least-privilege access remain key opportunities for improvement.

Web application security continues to represent a significant proportion of testing activity, with authentication, access control, and input validation issues regularly identified across client engagements.

Overall, the trends observed during Q2 2026 are consistent with previous quarters, highlighting the need for organisations to maintain a proactive approach to vulnerability management, secure application development, and identity security to reduce their overall attack surface.

Want to know more?

iSTORM remains committed to helping clients strengthen their security posture by identifying vulnerabilities before they can be exploited and by providing practical, risk-based recommendations to support ongoing cyber resilience. to find out more, or how we can help, get in touch today.

How can we help?



As a boutique 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