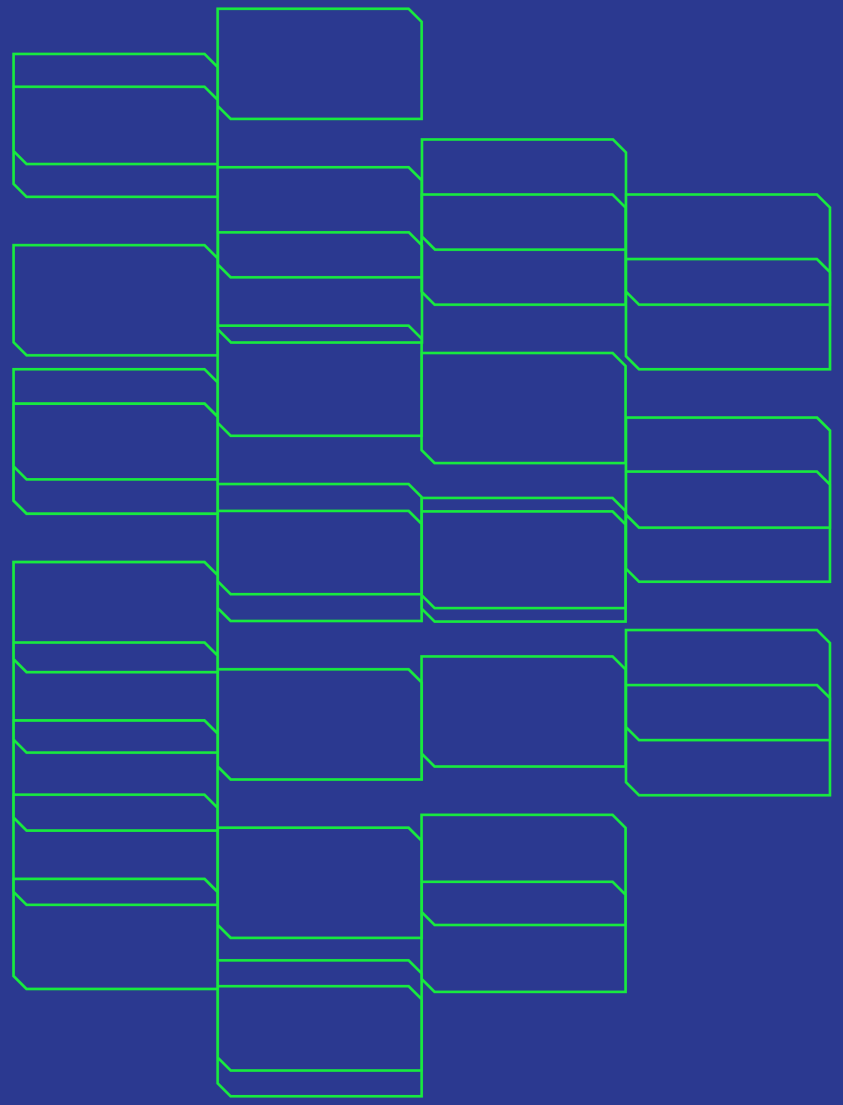
Security .Days

<Utrecht.NL>
<7-9 April 2026>

GÉANT

The national picture of risk: two years of UK ASM results

Iain Brown (Jisc)



Co-funded by
the European Union

Project background: A snapshot of sector vulnerability and resilience

Aim: To understand the sector's challenges and reduce cyber risks.

Objective: Passively scan the entire .ac.uk namespace, identify all Internet-facing assets at a set point in time, and record common technologies, services and risks.

- October 2024: 1,284 organisations across FE, HE, Research and related sectors
- August 2025: 1,263 organisations

Scanning statistics

1,263 organisations

Sector	No. of orgs	No. of domains
Further Education	541	1,583
Higher Education	314	3,209
Research	119	518
Others	294	495
Total	**1,263**	**5,805**

Findings from 5,805 input domains:

- 54,000 IP addresses
- 197,000 domains and subdomains
- 116,000 websites – only 52,000 are active
- 281,000 online services
- 193,000 risks:
  - 7,750 critical-severity risks
  - 47,000 high-severity risks
  - 138,000 medium-severity risks

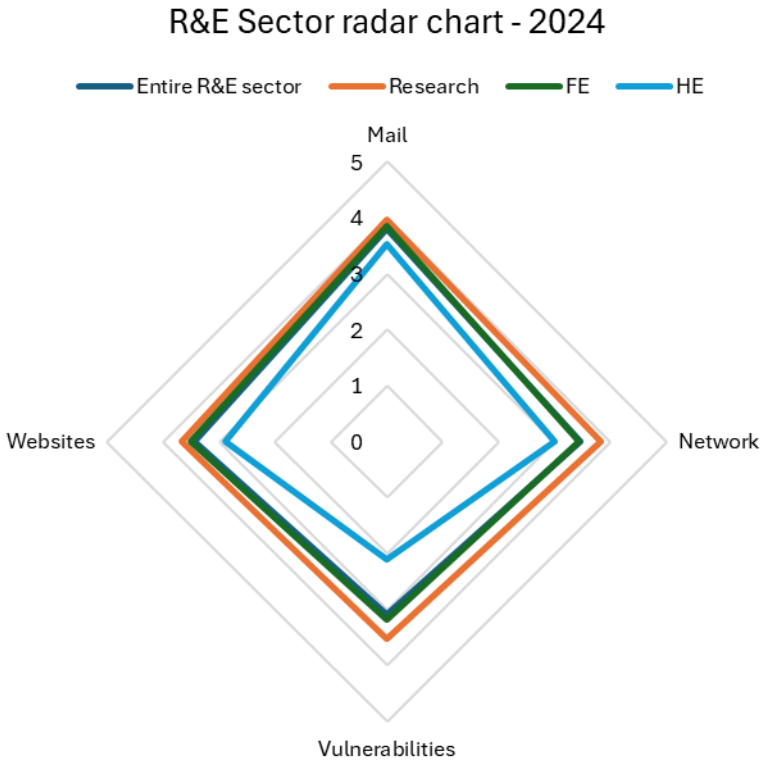
Comparison with 2024's scan results

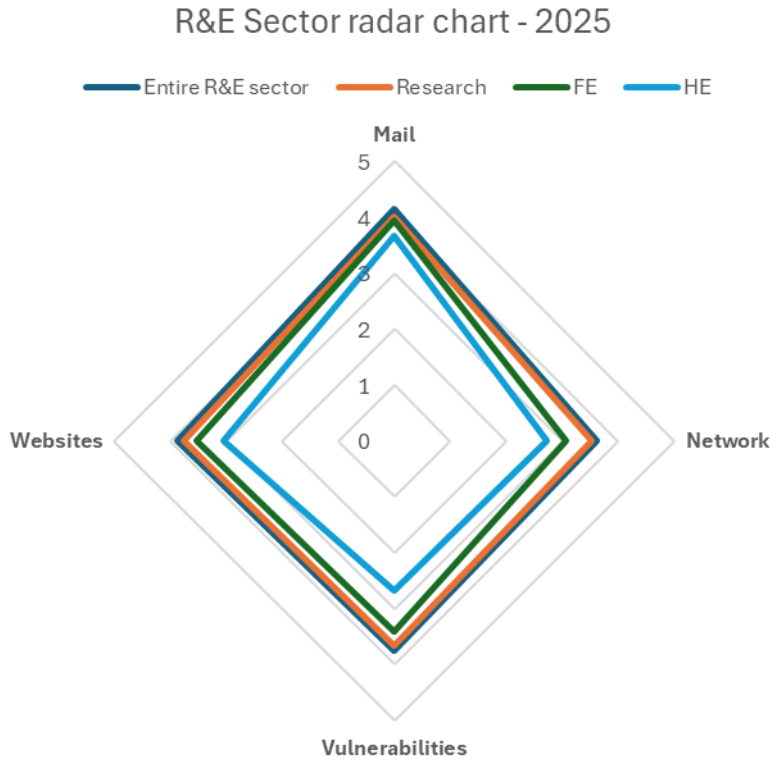
	2024	Baseline: % of 2024 Total Assets		2025	Baseline: % of 2025 Total Assets		Percentage point change
No. of organisations	1,284	–		1,263	–		-1.6% decrease
No. of input domains	5,707	–		5,805	–		1.7% increase
Total Assets	641,450	100		651,204	100		0
Live domains	195,973	31		198,691	31		0
IP addresses	53,173	8		54,094	8		0
Services	273,721	43		281,480	43		0
Websites	118,583	18		116,939	18		0
Critical-severity vulns	10,991	2		7,846	1		-1
High-severity vulns	37,409	6		47,767	7		1
Medium-severity vulns	213,174	33		139,164	21		-12

Comparison with other sectors

Sector	Average no. of assets	Average no. of Critical, High, Med severity risks	Average no. of Risks per Asset
Airlines	752.8	121.6	0.1615
Supermarkets	1,398.4	125.2	0.0895
Utility companies	647.2	73.4	0.1134
Total sector	**523.9**	**156.6**	**0.2911**
Further Education	143.1	39.2	0.2878
Higher Education	1,657.6	502.2	0.2890
↳ Research-intensive HE	9,567.1	2,810.6	0.3022
Research	302.0	79.1	0.2977

Health scores across all sectors

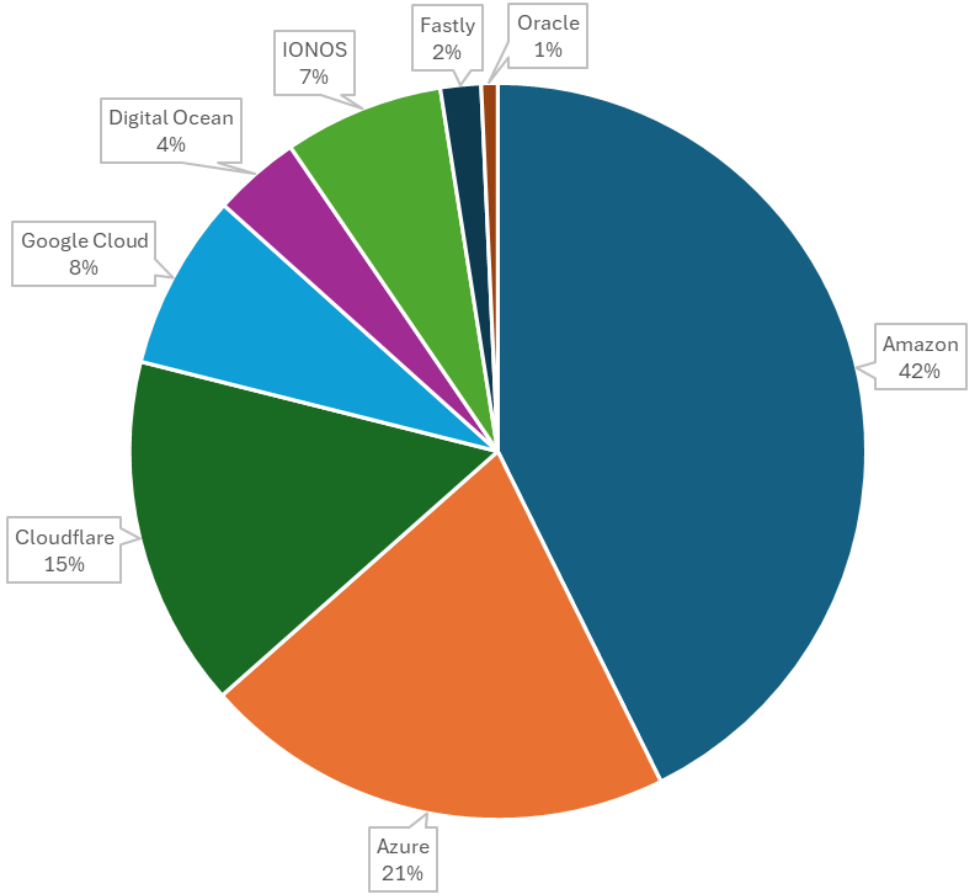




	2024	2025	Change	Improvement (%)
Overall Score: Mail	3.80	4.14	0.34	8.28
Overall Score: Network	3.47	3.63	0.16	4.47
Overall Score: Vulnerabilities	3.10	3.75	0.65	17.29
Overall Score: Websites	3.43	3.88	0.45	11.51
Overall Score	2.42	3.07	0.65	21.03

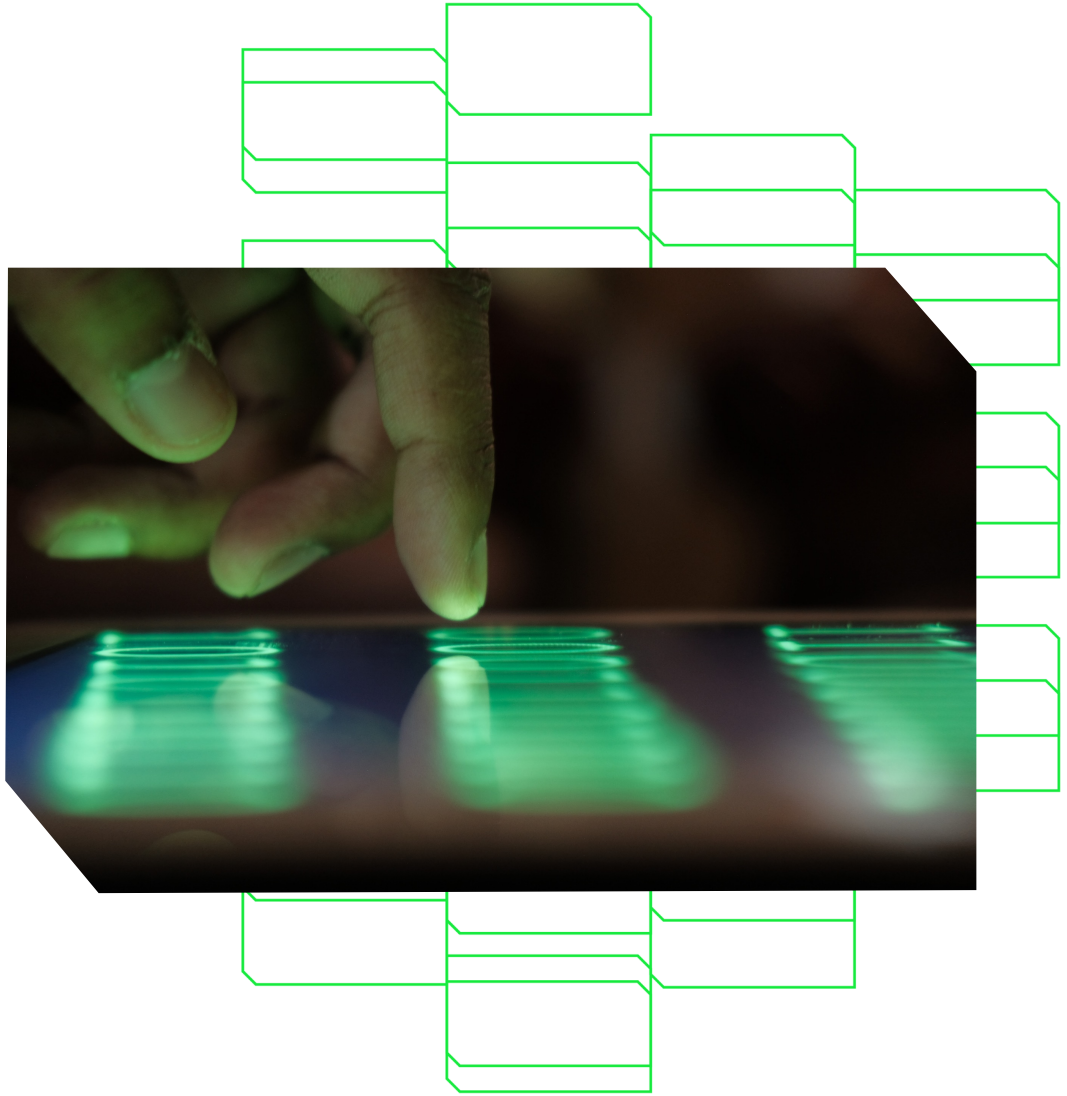
Cloud providers

Cloud region	Number	% of total
Amazon	2,777	43%
Azure	1,351	21%
Cloudflare	1,005	15%
Google Cloud	503	8%
IONOS	456	7%
Digital Ocean	249	4%
Fastly	116	2%
Oracle	47	1%
Akamai	18	<1%
Imperia	4	<1%



278,910 issues identified

- 84,000 TLS-related risks:
  - 54,000 TLS certificate issues
  - 12,000 vulnerable TLS protocols and cipher suites need removing
- 56,000 incorrect CSP configurations
- 48,000 poorly configured security headers
- 12,000 Websites available over HTTP
- 45,000 CVE vulnerabilities (critical, high and medium severity)
- 2,645 Known Exploitable Vulnerabilities
- 5,000 issues with SPF records
- 3,500 issues with DMARC records



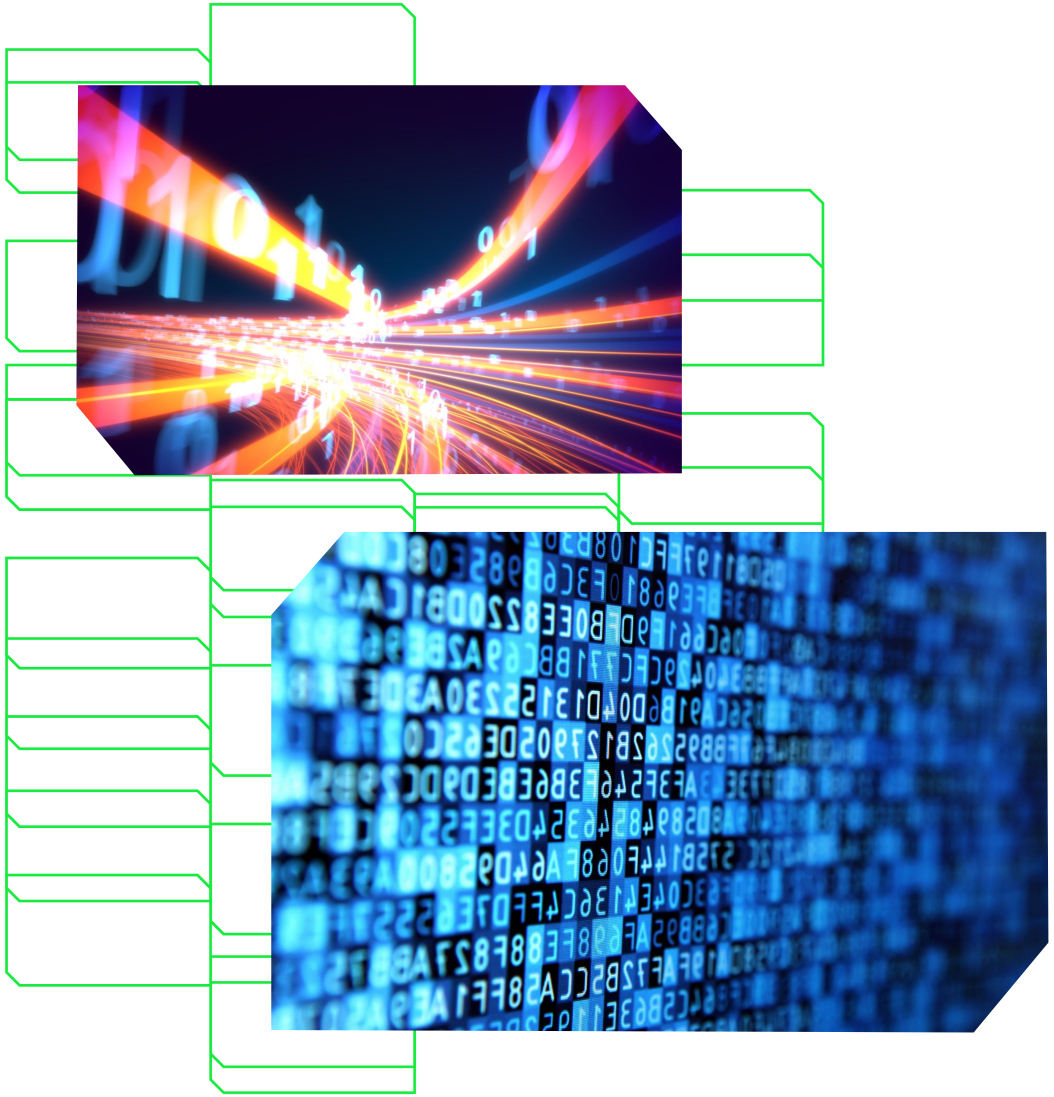
Most common vulnerabilities

18,000 critical- and high-severity vulnerabilities

Component	Count
PHP	10,189
WordPress	2,011
OpenSSL	1,717
nginx	1,032
Moment.js	743
MediaWiki	368
Lodash	361
Jetty	309
MathJax	210
Drupal	193
AngularJS	174

Vulnerability	Count	Impacts
CVE-2024-3566	942	Windows apps
CVE-2017-8923	269	PHP
CVE-2022-37454	150	PHP
CVE-2022-2068	149	OpenSSL
CVE-2025-1861	142	PHP
CVE-2019-9641	142	PHP
CVE-2024-8932	136	PHP
CVE-2024-11236	136	PHP
CVE-2019-9020, -9021, -9023 (each)	113	PHP
CVE-2019-6977	113	PHP

Three quick wins



1. **Web:**
    1. Update vulnerable components
    2. Fix HTTP headers
    3. Address TLS vulnerabilities
2. **Email:**
    1. SPF
    2. DKIM
    3. DMARC
3. **Disable / filter:**
    1. SSH
    2. FTP
    3. Telnet
    4. RDP
    5. SMB

Any questions?

Co-funded by
the European Union