HEALTHCARE / AZURE CRITICAL

Patient Records Exposed to the Public Internet for 18 Months

CVSS 9.8 | Found in week one, by hand

01 Engagement Overview

A healthcare provider running its patient infrastructure on Azure engaged DivIHN for an external and cloud-focused penetration test after 18 months of clean monthly vulnerability scans, believing its security posture was strong.

- Scope: Internet-facing Azure assets, storage environment, API layer, and patient portal.
- Approach: Black-box reconnaissance, storage account enumeration, and manual configuration review.
- Baseline: Monthly automated vulnerability scans, with no prior findings.

02 Technical Discovery

Within the first week, manual enumeration of the client's Azure Blob Storage accounts identified a container configured for anonymous public read/list access instead of private access. Anyone with the URL could access its contents.

- Exposed: Patient names, dates of birth, diagnosis codes, insurance identifiers, and unencrypted patient data.
- Root cause: Automated vulnerability scanners primarily assess CVEs, exposed ports, and known vulnerabilities rather than the client's storage IAM and ACL configuration.
- This class of misconfiguration surfaced during manual configuration review against CIS Azure Benchmarks.

03 Risk & Business Impact

The finding received a CVSS score of 9.8, placing it in the Critical severity category and indicating a remotely exploitable, zero-privilege path to sensitive PHI.

- HIPAA: The exposure may trigger HIPAA breach of notification and reporting obligations, depending on the nature and scope of the compromised PHI.
- The exposure could also lead to HHS Office for Civil Rights scrutiny and potential civil monetary penalties, depending on the circumstances.
- Eighteen months of clean automated scans followed by a week-one manual discovery demonstrated the limitations of relying on compliance-driven vulnerability scanning alone.

04 Remediation & Outcome

DivIHN worked with the client's cloud engineering team to eliminate the public exposure and strengthen the surrounding storage environment against similar misconfigurations.

- Changed the container's access configuration to private and added Azure Storage firewall rules.
- Moved integrations to short-lived SAS tokens.
- Enabled Microsoft Defender for Storage to detect and flag future anonymous access changes.
- Instituted quarterly manual cloud configuration reviews alongside the existing automated scans.