

THE PATCH WAS AVAILABLE. THE OWNER WASN'T.

A state-sponsored campaign breached university mail servers using Roundcube vulnerabilities that were fixed months before the first phishing email went out.

Both fixes existed before the campaign began.

CVE-2024-42009

CROSS-SITE SCRIPTING

CVSS

9.3

PATCHED 2024

CVE-2025-49113

REMOTE CODE EXECUTION

CVSS

9.9

PATCHED JUN 1, 2025



Discovery Problem vs. Ownership Problem

	FRIDAY'S FN	SATURDAY'S FN
Failure type	Discovery problem	Ownership problem
Vulnerability	New	Existing
Core question	Can defenders find it fast enough?	Was anyone responsible for it?
Patch window	Just opened	Ignored for months

Two Vulnerabilities, Chained



IceCube (JS payload) harvests session credentials and 2FA cookies. SquareShell / VShell drop as the webshell; SNOWLIGHT is the fallback loader.

Eleven Months of Exposure



The remediation deadline that existed still didn't reach university mail servers — it bound federal civilian agencies, not higher education.

Not Indiscriminate. Deliberately Narrow.

< 10

CONFIRMED VICTIMS
(DOZENS SUSPECTED)

Physics and engineering departments, specifically

National-security-linked or astrophysics/particle-physics research

Individual departments legitimately run their own infrastructure — distributed ownership, not negligence

That ownership rarely carries patch responsibility with it

Every Org Has One of These

1 Internal Git server someone spun up years ago

2 Legacy Jenkins box nobody's touched since

3 Monitoring appliance that alerts on everything except its own patch level

4 Backup console with admin access to what you can't afford to lose

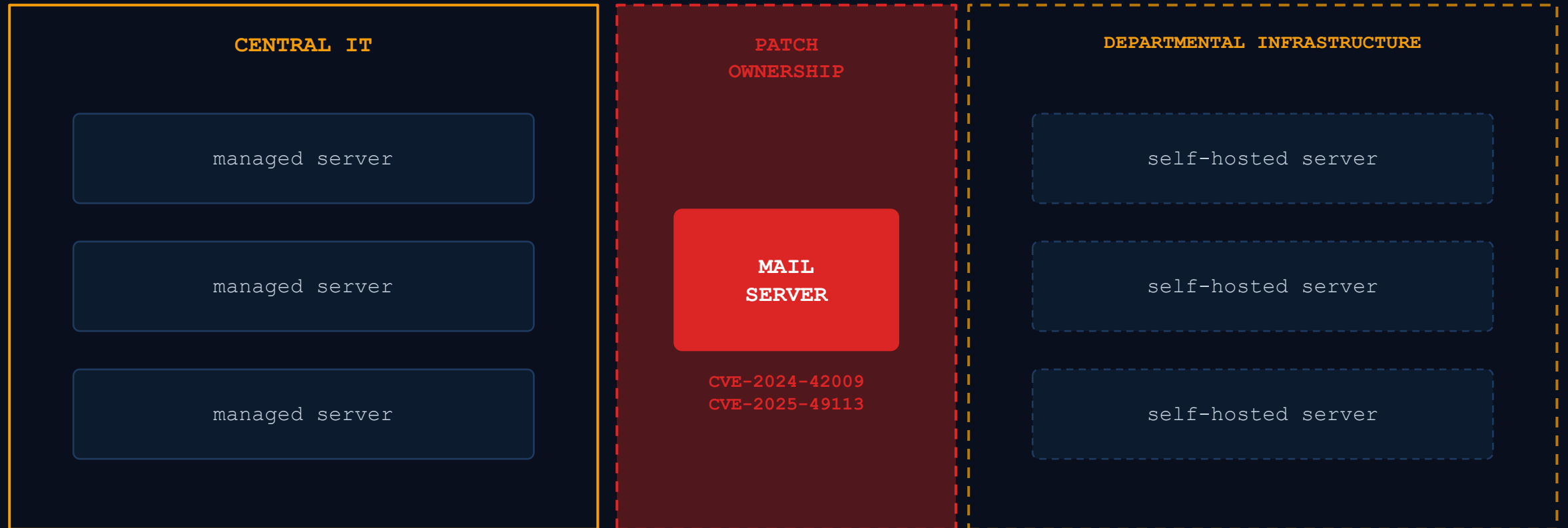
5 Forgotten management VM still holding valid credentials

6 Department-run Kubernetes cluster off the platform team's radar

Patchable. Legitimate. Unowned.



Between Two Legitimate Owners



Fixes Are Cheap. Ownership Is the Expensive Part.

Infrastructure rarely stays vulnerable because fixes don't exist. It stays vulnerable because responsibility is fragmented.

rack2cloud.com | Follow The Architect for more