MODERN INFRASTRUCTURE & IaC

Patch Rollback Risk

When Recovery Reintroduces the Exposure You Just Closed

Microsoft's September 2026 RDS failure exposed a common architecture problem: restoring service restoring service can reverse the remediation that made the service secure.

The Failure

THREE CUMULATIVE UPDATES

KB5122876	Windows Server 2019
KB5122882	Windows Server 2022
KB5122871	Windows Server 2025

REPORTED BEHAVIOR

- Sessions fail to disconnect
- New connections hang
- RDS becomes unavailable

Availability failed after remediation succeeded.

THE CORE PROBLEM

No State Is Automatically Safe

STATE	SECURITY	AVAILABILITY
Patched	Protected	Normal
Failed	Protected	Broken
Rolled Back	Vulnerable	Restored

No state is automatically “safe.”

Recovery restores service.

Recovery also removes the remediation.

Rolling back the update can reintroduce **CVE-2026-69525**, a critical RDS remote-code-execution vulnerability.

Can we roll back?

Any administrator can uninstall an update.

THE REAL QUESTION IS:

Who is authorized to reverse a remediation?

The Rollback Authority Model

01

Who owns the decision?

02

What evidence is required?

03

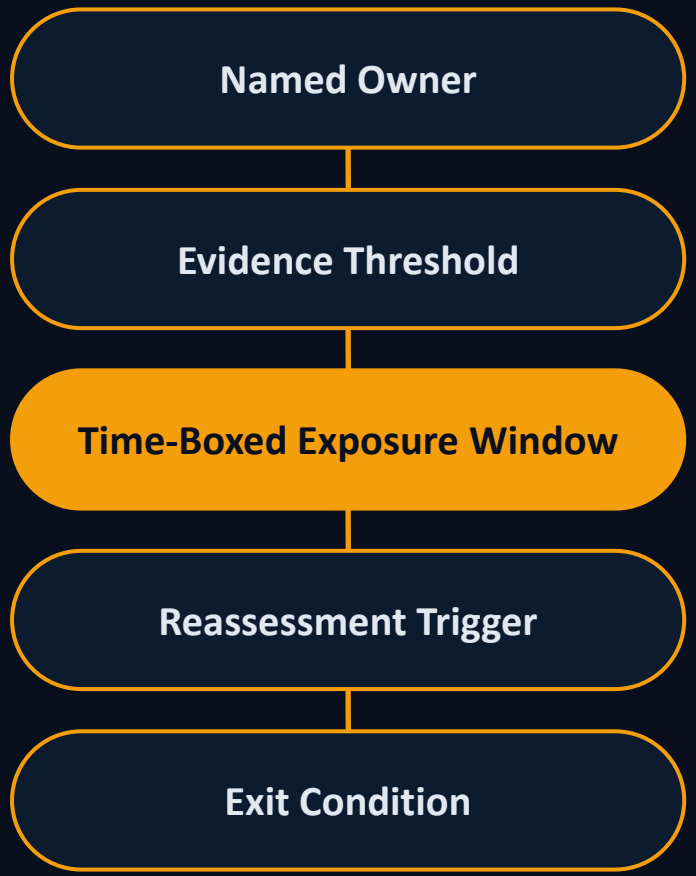
How long may exposure remain?

04

What information channels are available?

Authority without evidence is guesswork. Evidence without authority is delay.

The Runbook Chain



A rollback should be a controlled exception, not a new operating state.

ARCHITECT'S VERDICT

“Security-complete and operationally-safe are not the same claim.”

Patch rollback risk appears when remediation and recovery become competing objectives.

rack2cloud.com | Follow The Architect for more