maze

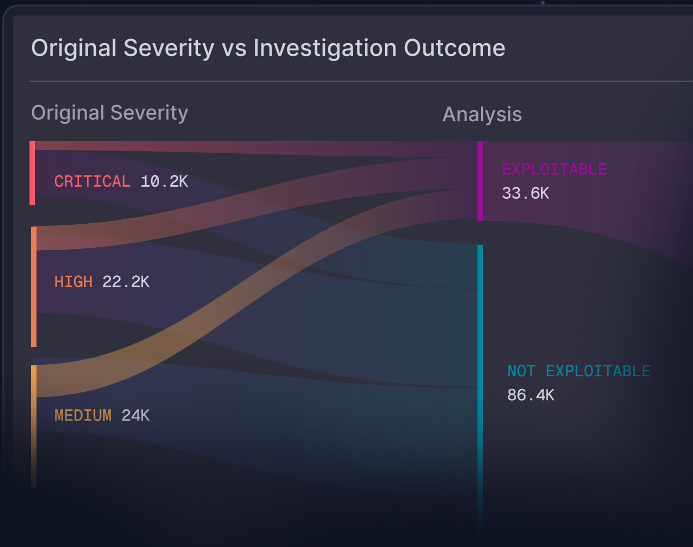
Get Cloud Vulnerabilities Under Control

AI agents that investigate, triage, and remediate cloud vulnerabilities like expert security engineers.

Maze investigates every vulnerability in your cloud environment to determine what's actually exploitable, not just what's potentially risky.

Our AI agents act like expert security engineers: validating if exploitation is possible, analyzing attack paths, assessing business impact, and assisting remediation.

Stop wasting time on vulnerabilities that can't hurt you and speed up remediation for the few that can.



Original Severity vs Investigation Outcome

Feeling Vulnerable? Focus on Real Risks, Not False Alarms

AI Agents Delivering Real Results to Security Teams

- Eliminate 95% of your vulnerability backlog
- Automate remediation workflows
- One-click compliance reporting for not-exploitable findings, with a full audit trail

> “Maze understands what's exploitable in our environment, not just CVSS/EPSS, but truly exploitable. That's what set Maze apart from every other vendor.”

Jonathan Mattey
Chief Information Security Officer
Forge Holiday Group

Prove What’s Not Exploitable

- Each asset is independently investigated to determine if exploitation is technically possible
- Runtime context, configuration, compensating controls, and dependencies are analyzed
- Findings are marked exploitable or not exploitable with a full audit trail

Prioritize Based on Actual Risk

- Exploitation difficulty is evaluated in depth
- Blast radius and business impact are assessed
- Vulnerabilities are prioritized with human level precision, not generic scores or rule engines

Stop Project Managing Remediation

- Root cause is identified and issues grouped
- Owners are found and intelligent fixes suggested
- Vulnerabilities are fixed faster with less effort

Exploitability-First Vulnerability Analysis

Maze ingests findings from your existing cloud scanners and investigates each one to determine whether exploitation is technically possible in your environment. No manual triage required.

Prioritize With Human-Level Precision

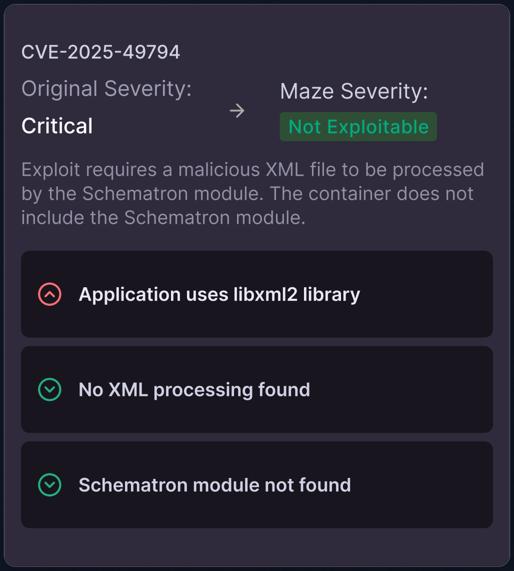
Maze's AI agents assess business and technical context to prioritize the few vulnerabilities that pose real risk to your organization.

Agentless Deployment with Runtime Context

Maze gathers the runtime data required for investigation directly from your cloud environment and workloads, across virtual machines and containers, without deploying agents or sensors.

Stop Project Managing Remediation

AI agents manage remediation end-to-end: identifying root cause, finding owners, and suggesting fixes. Engineering gets clear, actionable guidance.

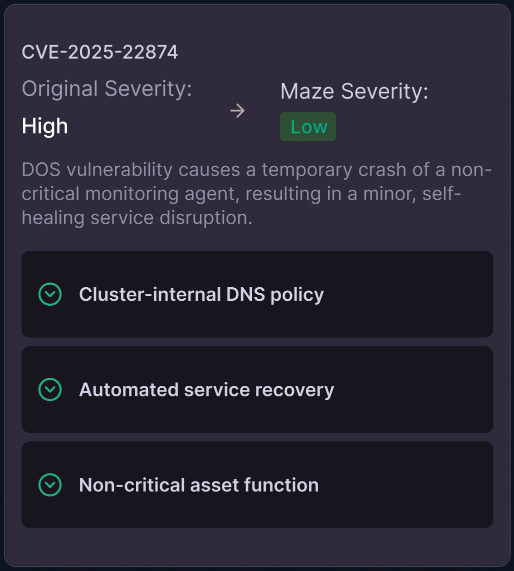


CVE-2025-49794

Original Severity: Critical → Maze Severity: Not Exploitable

Exploit requires a malicious XML file to be processed by the Schematron module. The container does not include the Schematron module.

- Application uses libxml2 library
- No XML processing found
- Schematron module not found

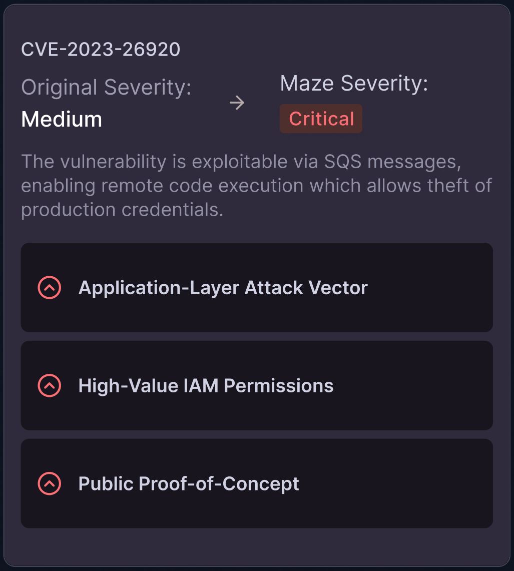


CVE-2025-22874

Original Severity: High → Maze Severity: Low

DOS vulnerability causes a temporary crash of a non-critical monitoring agent, resulting in a minor, self-healing service disruption.

- Cluster-internal DNS policy
- Automated service recovery
- Non-critical asset function



CVE-2023-26920

Original Severity: Medium → Maze Severity: Critical

The vulnerability is exploitable via SQS messages, enabling remote code execution which allows theft of production credentials.

- Application-Layer Attack Vector
- High-Value IAM Permissions
- Public Proof-of-Concept

About Maze

Maze delivers AI-native cloud vulnerability management that cuts through the noise. We investigate every vulnerability to reveal what's actually exploitable, letting security teams focus on what matters instead of drowning in alerts. Founded in 2024 with $31M in funding, Maze is trusted by fast-growing companies to manage vulnerabilities with clarity and speed.

> "Maze does the triaging for us so that we don't have to... I'm happy to report, Maze was accurate, and we are confident in the solution."

Nathan Cooke
Manager of Product Security
ALLOY

Ready to stop drowning in vulnerability noise?

Book a demo → mazehq.com/demo