NATIONAL CSIRT CY

CVE-2025-45569

02/05/2025

Open Policy Agent HTTP Data API Path Injection Leading to Rego Code Execution (CVE-2025-46569)

CONFIDENTIAL

Executive Summary

CVE-2025-46569 is a high-severity vulnerability in Open Policy Agent (OPA) versions prior to 1.4.0 that allows attackers to inject Rego policy code through specially crafted HTTP Data API request paths. This can result in unauthorized policy behavior, potential data leakage, or denial of service. The issue has been fixed in OPA version 1.4.0, and users are strongly advised to upgrade immediately and restrict access to the OPA API.

Analysis

The vulnerability lies in how Open Policy Agent (OPA) handles HTTP Data API paths. In affected versions (prior to 1.4.0), the request path is not properly sanitized before being processed in policy evaluation. This allows an attacker to inject Rego code via the URL path, potentially altering policy behavior or executing unintended logic.

The core issue stems from insufficient input validation, enabling injection into dynamically generated Rego queries. This could be exploited to craft malicious queries that:

- Bypass intended policy checks
- Leak sensitive decision-making data (oracle attacks)
- Consume excessive resources (DoS)

Common Vulnerabilities & Exposures

https://nvd.nist.gov/vuln/detail/CVE-2025-46569

Versions affected

- **All versions prior to 1.4.0**

Solutions

To resolve CVE-2025-46569, users should upgrade Open Policy Agent (OPA) to version 1.4.0 or later, which addresses the vulnerability by properly sanitizing request paths. It is also recommended to restrict access to the OPA Data API to trusted networks, enforce strict authorization policies, and avoid including untrusted input in request paths.

Please distribute this information among your subsidiaries and partners, and also share with us any pertinent information and findings you may have (e.g IOCs, TTPs etc)

The Digital Security Authority extends its appreciation for the continued collaboration.

Disclaimer

Organizations are advised to consult with relevant cybersecurity professionals and follow best practices for their specific environments.