مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

DoS Vulnerability in Redis

Tracking #:432317463

Date:08-07-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a high-severity vulnerability (CVE-2025-48367) has been identified in Redis, affecting all versions of the popular in-memory data structure store.

TECHNICAL DETAILS:

A high-severity vulnerability (CVE-2025-48367) has been identified in Redis, affecting all versions of the popular in-memory data structure store. The issue arises from improper error handling in unauthenticated client connections, which can cause repeated IP protocol errors. These malformed or malicious connections ultimately exhaust Redis client resources, resulting in client starvation and denial of service (DoS).

The vulnerability requires no authentication, no privileges, and no user interaction, making it a serious threat for publicly exposed Redis instances. Patch releases have been issued in branches 6.2.x, 7.2.x, 7.4.x, and 8.0.x.
.

Vulnerability Details:

- CVE ID: CVE-2025-48367
- Package: redis-server
- Affected Versions: All versions (prior to patch)
- Patched Versions: Redis 6.2.X, 7.2.X, 7.4.X, 8.0.X
- CVSS Score: 7.5 (High)
- CVSS Vector:CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
- Technical Impact:
  - Unauthenticated connections cause IP protocol errors.
  - Triggers client starvation, preventing new clients from connecting.
  - Leads to complete denial of service without needing valid credentials.
- Associated Weakness:
  - CWE-770: Allocation of Resources Without Limits or Throttling

Patches:

- Redis 6.2.X, 7.2.X, 7.4.X and 8.0.X

RECOMMENDATIONS:

- Upgrade Redis to one of the patched version.
- Enforce **strong authentication** and avoid exposing Redis instances to untrusted networks.
- Review Redis security best practices to harden deployments against authenticated abuse.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://github.com/redis/redis/security/advisories/GHSA-4q32-c38c-pwgq