مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

RCE Vulnerability in Redis

Tracking #:432317930

Date:04-11-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Redis, the widely used in-memory data platform, has issued an urgent patch addressing a high-severity remote code execution (RCE) vulnerability.

TECHNICAL DETAILS:

Redis, the widely used in-memory data platform, has issued an urgent patch addressing a high-severity remote code execution (RCE) vulnerability identified as CVE-2025-62507.

The issue lies in the XACKDEL command, used in stream message acknowledgment and deletion, which can be exploited to trigger a stack buffer overflow under specific conditions. Successful exploitation could allow an authenticated attacker to execute arbitrary code within the Redis server process, potentially compromising the entire host system.

Vulnerability Details:

- CVE ID: CVE-2025-62507
- Severity: High
- CVSS v4 Base Score: 7.7
- Affected Versions: Redis >= 8.2.0
- Fixed Version: Redis 8.2.3
- Vulnerability Type: Stack Buffer Overflow → Remote Code Execution (RCE)
- Attack Vector: Network (Authenticated via CLI or API)

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade Redis to fixed version or later as soon as possible.

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-jhjx-x4cf-4vm8