مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Critical Remote Code Execution Vulnerability in Redis

Tracking #:432317785

Date:07-10-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that the Redis security team has issued an urgent patch for a critical remote code execution (RCE) vulnerability (CVE-2025-49844) that affects all Redis versions.

TECHNICAL DETAILS:

The Redis security team has issued an urgent patch for a critical remote code execution (RCE) vulnerability (CVE-2025-49844) that affects all Redis versions.

This flaw stems from a 13-year-old use-after-free vulnerability in the Lua scripting engine, which is enabled by default in Redis. Successful exploitation allows authenticated attackers to escape the Lua sandbox, execute arbitrary code, and gain full control of the host system.

The vulnerability, dubbed "RediShell" by Wiz researchers, impacts both Redis Enterprise and Redis OSS/Community editions.

Given the widespread use of Redis in cloud and enterprise environments, and with over 330,000 instances exposed online (including 60,000 without authentication), the risk of exploitation is extremely high.

Organizations using Redis must apply patches immediately and secure all instances exposed to the internet to prevent compromise, data theft, or cryptocurrency mining abuse.

Vulnerability Details

- **CVE Identifier:** CVE-2025-49844
- **CVSS Score 10.0** (Critical)
- An authenticated user may use a specially crafted Lua script to manipulate the garbage collector, trigger a use-after-free and potentially lead to remote code execution.

Impacted releases	Fixed releases
All Redis Software releases	7.22.2-12 and above, 7.8.6-207 and above, 7.4.6-272 and above, 7.2.4-138 and above, 6.4.2-131 and above
All Redis OSS/CE/Stack releases with Lua scripting	OSS/CE: 8.2.2 and above, 8.0.4 and above, 7.4.6 and above, 7.2.11 and above, Stack: 7.4.0-v7 and above, 7.2.0-v19 and above

RECOMMENDATIONS:

- **Apply Security Patches**
  - Upgrade Redis to the latest patched versions listed above.
  - Prioritize patching all internet-facing or publicly accessible instances.
- **Restrict Access**
  - Enable authentication for all Redis deployments.
  - Restrict Redis access to trusted IPs or internal networks only.
  - Implement firewall or VPC rules to prevent external connections

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://redis.io/blog/security-advisory-cve-2025-49844/