مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical Remote DoS Vulnerability in Apache bRPC

Tracking #:432317592

Date:12-08-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in Apache bRPC's Redis protocol parser that could allow remote attackers to crash services via memory exhaustion.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2025-54472**
- The vulnerability stems from improper memory allocation in the Redis protocol parser. When parsing incoming network data, the parser allocates memory for arrays and strings based on integer values. If a malicious actor sends a specially crafted Redis packet with an excessively large integer, it can trigger uncontrolled memory allocation, leading to a crash (Denial-of-Service).
- **Component Affected**: Redis Protocol Parser in Apache bRPC
- **Affected Versions**: All versions prior to 1.14.1
- **Fixed Version**: 1.14.1

Exploitable Scenarios:

- bRPC as a Redis Server: Accepting connections from untrusted clients.
- bRPC as a Redis Client: Connecting to untrusted Redis services.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the fixed updates or patch at the earliest.

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://lists.apache.org/thread/pvw31sxjj1yz0f8f8lp9m09h70w9hnct