

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



RCE Vulnerability in Apache bRPC
Tracking #:432318273
Date:20-01-2026

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 INTELLIGENCE 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 that Apache bRPC contains a remote command injection vulnerability in its heap profiler built-in service. An unauthenticated attacker can exploit insufficient input validation to execute arbitrary commands on affected systems.

TECHNICAL DETAILS:

A remote command injection vulnerability in Apache bRPC's heap profiler built-in service (/pprof/heap). The issue allows an attacker to inject and execute arbitrary commands through the extra_options parameter.

Vulnerability Details

- **CVE-2025-60021**
- Severity: important
- Apache bRPC's heap profiler built-in service (/pprof/heap) accepts a user-supplied parameter named extra_options. The service does not validate or sanitize this input and passes it directly as a command-line argument. As a result, an attacker can craft malicious input to execute arbitrary commands on the host running the bRPC service.
- This vulnerability affects all platforms where Apache bRPC is deployed and is exploitable remotely if the /pprof/heap endpoint is accessible.

Affected Versions

- Apache bRPC 1.11.0 before 1.15.0

Fixed Versions

- Apache bRPC 1.15.0 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Apache.

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://nvd.nist.gov/vuln/detail/CVE-2025-60021>