CVE-2025-21605: REDIS DOS VIA UNAUTHENTICATED CLIENT OUTPUT BUFFER ABUSE

Vairav CVE Report

Date: April 24, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

Redis has disclosed a high-severity denial-of-service (DoS) vulnerability (CVE-2025-21605) affecting versions 2.6 and later. An unauthenticated remote attacker can trigger uncontrolled memory consumption by abusing Redis's output buffer via repeated NOAUTH responses. The flaw can cause service crashes or system memory exhaustion. Immediate mitigation is advised.

VULNERABILITY DETAILS

CVE-2025-21605: Redis DoS via Unauthenticated Client Output Buffer Abuse

Description: Redis does not limit output buffer growth for normal clients by default. An unauthenticated client, by repeatedly triggering authentication errors, can exhaust memory resources over time, resulting in a denial of service.

Impact: Remote, unauthenticated attackers can cause service downtime or force Redis to be killed due to out-of-memory conditions.

CVSS Score: 7.5 (High)

AFFECTED PRODUCTS/VERSIONS

- **Product**: redis-server
- **Affected Versions:** Version 2.6 and above
- **Patched Versions:** TBD (fix to be released)

EXPLOIT DETAILS

Attackers exploit this issue by connecting to a Redis instance with authentication enabled and sending continuous requests that elicit “NOAUTH” responses. These error responses are stored in the client output buffer, which can grow without limits and eventually exhaust system memory.

RECOMMENDATIONS

- **Upgrade Restrict access:** Use firewalls, iptables, or cloud security groups to block unauthenticated access.
- **Enable TLS and client certificate authentication**: Ensure only authorized clients can connect.

- **Set output buffer limits**: Configure client-output-buffer-limit to enforce memory thresholds for normal clients.
- **Monitor for abnormal memory usage**: Use Redis monitoring tools to detect suspicious activity.

REFERENCES

https://securityonline.info/redis-vulnerability-exposes-servers-to-denial-of-service-attacks/

https://www.cve.org/CVERecord?id=CVE-2025-21605

https://github.com/redis/redis/releases/tag/7.4.3

https://github.com/redis/redis/security/advisories/GHSA-r67f-p999-2gff

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com