Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Redis Under Siege: RediShell Flaw Opens Door to Remote Code Execution

Date of Publication	Admiralty Code	TA Number
October 9, 2025	A1	TA2025308

Summary

Discovered On: May 16, 2025
Affected Products: All Redis Software releases
Impact: A critical flaw, known as RediShell (CVE-2025-49844), has exposed Redis to a serious remote code execution risk stemming from a 13-year-old use-after-free bug. By sending a malicious Lua script, an authenticated attacker can escape the Lua sandbox and gain full control of the host system, potentially stealing credentials, deploying malware, and moving laterally across connected environments. While Redis Cloud has already patched the issue, self-managed users must upgrade immediately and secure their instances by upgrading to the latest patched version.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-49844	RediShell (Redis Remote Code Execution Vulnerability)	All Redis Software releases with Lua scripting	✗	✗	✓

Vulnerability Details

#1

A critical remote code execution vulnerability tracked as CVE-2025-49844, informally called RediShell, has been discovered in the widely used Redis in-memory data store. Redis is an open-source, in-memory data store used as a database, cache, and message broker for fast data access and real-time applications. The flaw lets an authenticated user submit a malicious Lua script that manipulates Redis's garbage collector, triggers a long-standing use-after-free memory corruption, and ultimately escapes the Lua sandbox to execute native code on the host.

#2

Technically, this is a use-after-free bug that appears to have been present in the Redis source code for roughly 13 years. Because Redis ships with Lua scripting enabled by default, a post-authentication attacker can craft a script that abuses the vulnerability to break out of the confined runtime and run arbitrary machine code with the privileges of the Redis process, a direct path from script to system compromise.

#3

The attacker typically uses the sandbox escape to spawn a reverse shell, then harvests credentials and secrets, for example, SSH keys, IAM tokens, and certificates from both Redis and the underlying host. From there, they can drop malware (including crypto-miners), exfiltrate sensitive data, and reuse stolen cloud credentials to pivot into additional services and accounts, amplifying damage across the environment.

#4

If you use Redis Cloud, the provider has already applied the fixes, and no user action should be necessary. If you self-manage Redis (Community or Software), immediately upgrade to the latest patched release. As short-term mitigations, consider restricting access to Redis instances, disabling or limiting Lua scripting where possible, rotating exposed credentials and tokens, checking logs for suspicious activity, and performing a review for indicators of compromise.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-49844	All Versions of Redis with Lua Scripting (Before 8.2.2)	cpe:2.3:a:redis:redis:*:*:*:*:*:*:*:*	CWE-416

Recommendations

Immediate Action: If you’re using Redis Cloud, the service provider has already rolled out patches addressing CVE-2025-49844 (RediShell). However, it’s still important to review recent activity logs and verify there are no signs of unusual behavior. For self-managed Redis deployments (Community or Software versions), upgrade to the latest patched release without delay.

Restrict Network Access: Ensure Redis instances are not exposed to the internet. Place them behind a firewall or within a private network and limit access only to trusted applications or IP addresses.

Enable Detailed Logging: Improve visibility by enabling advanced logs and configuring alerts for suspicious Lua activity or unauthorized system access.

Enforce Strong Authentication: Always require authentication for every connection to Redis. Avoid running instances with open or unauthenticated access, as this leaves them vulnerable to exploitation and data exposure. Ensure Protected Mode is enabled so Redis only accepts connections from trusted hosts by default.

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0008 Lateral Movement	TA0010 Exfiltration
T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1059 Command and Scripting Interpreter	T1497 Virtualization/Sandbox Evasion
T1552 Unsecured Credentials	T1552.001 Credentials In Files	T1068 Exploitation for Privilege Escalation	T1021 Remote Services

Patch Details

Upgrade to the latest Patched Versions.

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.

Redis OSS/CE/Stack releases with Lua scripting: 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.

Links:
https://github.com/redis/redis/releases/tag/8.2.2

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

References

https://www.wiz.io/blog/wiz-research-redis-rce-cve-2025-49844

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

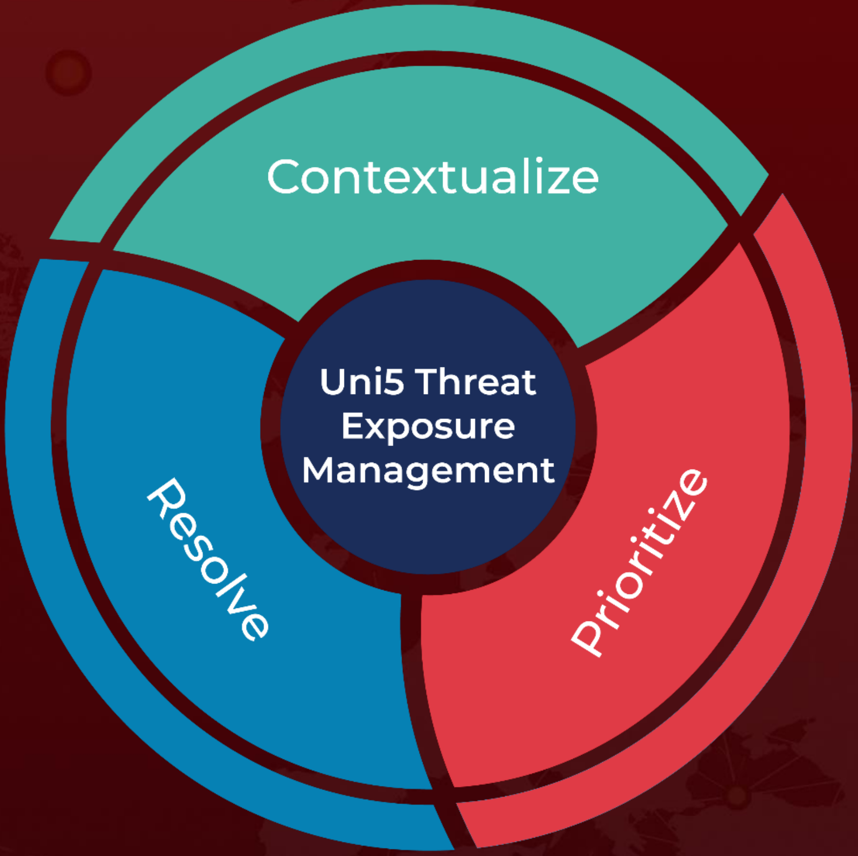
https://github.com/redis/redis/security/advisories/GHSA-4789-qfc9-5f9q

https://github.com/raminfp/redis_exploit/blob/main/exploit_poc.py

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

October 9, 2025 • 2:30 AM

More at www.hivepro.com