



NCSC-2025-0304

Kwetsbaarheden verholpen in Redis

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 08-10-2025

TLP:WHITE

Toegestane verspreiding van TLP:WHITE

(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Redis heeft kwetsbaarheden verholpen in versies 8.2.1 en lager.

Duiding

De kwetsbaarheden bevinden zich in de Lua-scriptingengine van Redis, die kunnen worden misbruikt door geauthenticeerde gebruikers. Dit kan leiden tot remote code execution, out-of-bounds data access of servercrashes. De kwetsbaarheden kunnen de integriteit en beveiliging van systemen die deze versies gebruiken in gevaar brengen. De kwetsbaarheden zijn opgelost in versie 8.2.2. Veel Redis-implementaties hebben geen pre-authenticatie of ACL-gebaseerde autorisatie ingeschakeld; dit vergroot het risico op exploitatie.

Onderzoekers hebben Proof of Concept (PoC) code vrijgegeven die kwetsbaarheid CVE-2025-49844 aantoont en waarmee de kwetsbaarheid kan worden misbruikt.

Oplossingen

Redis heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://github.com/redis/redis/releases/tag/8.2.2>
- <https://github.com/redis/redis/security/advisories/GHSA-4789-qfc9-5f9q>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-49844	5.3 MEDIUM
➤ CVE-2025-46817	7.3 HIGH
➤ CVE-2025-46818	2.0 LOW
➤ CVE-2025-46819	6.3 MEDIUM

CWE's

CWE	Beschrijving
> CWE-416	Use After Free
> CWE-190	Integer Overflow or Wraparound
> CWE-94	Improper Control of Generation of Code ('Code Injection')

Getroffen producten

Open Source
Redis
Redis
Redis

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.