NATIONAL CSIRT CY

CVE-2025-25186

11/02/2025

Net::IMAP Resource Consumption

CONFIDENTIAL

The content of this document is intended solely for use by the natural or legal person to whom it is addressed. If you gain access to this document by mistake, you should be aware that any forwarding, copying or disclosure of its content to any other person is strictly prohibited, and you must inform the sender immediately.

Executive Summary

A vulnerability, which was classified as problematic, was found in ruby net-imap up to 0.3.7/0.4.18/0.5.5. Affected is the function Net::IMAP. The manipulation with an unknown input leads to a resource consumption vulnerability. CWE is classifying the issue as CWE-400. The product does not properly control the allocation and maintenance of a limited resource, thereby enabling an actor to influence the amount of resources consumed, eventually leading to the exhaustion of available resources. This is going to have an impact on availability.

Analysis

Net::IMAP implements Internet Message Access Protocol (IMAP) client functionality in Ruby. Starting in version 0.3.2 and prior to versions 0.3.8, 0.4.19, and 0.5.6, there is a possibility for denial of service by memory exhaustion in `net-imap`'s response parser. At any time while the client is connected, a malicious server can send highly compressed `uid-set` data which is automatically read by the client's receiver thread. The response parser uses `Range#to_a` to convert the `uid-set` data into arrays of integers, with no limitation on the expanded size of the ranges. Versions 0.3.8, 0.4.19, 0.5.6, and higher fix this issue.

Additional details for proper configuration of fixed versions and backward compatibility are available in the GitHub Security Advisory.

Common Weakness Enumeration

https://cwe.mitre.org/data/definitions/400.html

Common Vulnerabilities & Exposures

https://nvd.nist.gov/vuln/detail/CVE-2025-25186

Affected Systems

Programming Language Software – Ruby - function Net::IMAP

0.3.0	**0.3.1**	**0.3.2**	**0.3.3**
0.3.4	**0.3.5**	**0.3.6**	**0.3.7**
0.4.0	**0.4.1**	**0.4.2**	**0.4.3**
0.4.4	**0.4.5**	**0.4.6**	**0.4.7**
0.4.8	**0.4.9**	**0.4.10**	**0.4.11**
0.4.12	**0.4.13**	**0.4.14**	**0.4.15**
0.4.16	**0.4.17**	**0.4.18**	**0.5.0**
0.5.1	**0.5.2**	**0.5.3**	**0.5.4**
0.5.5			

Solutions

Upgrading to version 0.3.8, 0.4.19 or 0.5.6 eliminates this vulnerability.

Please distribute this information among your subsidiaries and partners, and also share with us any pertinent information and findings you may have (e.g IOCs, TTPs etc)

The Digital Security Authority extends its appreciation for the continued collaboration.

Disclaimer

Organizations are advised to consult with relevant cybersecurity professionals and follow best practices for their specific environments.