مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Denial-of-Service Vulnerability in HAProxy

Tracking #:432317777

Date:06-10-2025

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 INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed HAProxy Technologies has disclosed and remediated a high-severity denial of service (DoS) vulnerability that impacts multiple HAProxy product lines.

TECHNICAL DETAILS:

HAProxy Technologies has disclosed and remediated a high-severity denial of service (DoS) vulnerability (CVE-2025-11230) that impacts multiple HAProxy product lines, including the Community Edition, Enterprise Edition, ALOHA appliances, and Kubernetes Ingress Controllers.

The flaw originates from an Inefficient Algorithm Complexity (CWE-407) in the mjson library, which HAProxy uses for JSON parsing. When HAProxy encounters specially crafted JSON requests containing extremely large numerical values, the process can be forced into a prolonged computation phase, eventually triggering the watchdog process to terminate HAProxy — resulting in service disruption.

Vulnerability Details

- CVE ID: **CVE-2025-11230**
- Severity: High
- CVSS v3 Base Score: 7.5
- The vulnerability stems from the mjson library used by HAProxy to parse JSON structures. When a request includes unusually large numerical values (e.g., 1e1000000000000000), the JSON parsing functions — particularly json_query(), jwt_header_query(), and jwt_payload_query() — consume excessive processing time. This condition results in HAProxy's watchdog mechanism terminating the process to prevent indefinite hangs, effectively allowing attackers to cause a denial of service through repeated malicious requests.

Product	Affected Branches	Fixed Version
HAProxy Community Edition	2.4, 2.6, 2.8, 3.0, 3.1, 3.2	2.4.30, 2.6.23, 2.8.16, 3.0.12, 3.1.9, 3.2.6
HAProxy Enterprise	hapee-2.4r1 → hapee-3.1r1	hapee-2.4r1-lb-1.0.0-294.1446, hapee-2.6r1-lb-1.0.0-301.1704, hapee-2.8r1-lb-1.0.0-327.1146, hapee-3.0r1-lb-1.0.0-346.795, hapee-3.1r1-lb-1.0.0-349.585
HAProxy ALOHA Appliance	14.5, 15.5, 16.5, 17.0	14.5.33, 15.5.28, 16.5.19, 17.0.7
HAProxy Kubernetes Ingress Controller	All versions	v3.1.12
HAProxy Enterprise Kubernetes Ingress Controller	All versions	v1.9.14-ee7, v1.11.12-ee10, v3.0.15-ee4

RECOMMENDATIONS:

- Immediate Mitigation: Upgrade to the latest fixed version for HAProxy product as listed above.

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.

REFERNCES:

- https://www.haproxy.com/blog/october-2025-cve-2025-11230-haproxy-mjson-library-denial-of-service-vulnerability