مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Exploited Vulnerability in HAProxy

Tracking #:432316237

Date:09-09-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in HAProxy that is being actively exploited by threat actors. This vulnerability can lead to a remote denial-of-service (DoS) attack by causing HAProxy to crash under certain conditions.

TECHNICAL DETAILS:

CVE-2024-45506 is a vulnerability found in HAProxy, a widely-used load balancing and proxy software. It has been confirmed to be actively exploited, posing a severe risk to high-availability services. The vulnerability affects the HTTP/2 multiplexer and can lead to system crashes and remote denial-of-service (DoS) attacks.

Vulnerability Details:

- **CVE-2024-45506**
- CVSS Score**: 7.5 (High)**
- The vulnerability is triggered by flaws in the HTTP/2 multiplexer's handling of zero-copy forwarding. An attacker exploiting this could create an endless loop in the h2_send() function, particularly when:
  - A GOAWAY frame is triggered incorrectly.
  - The output buffer is "full," preventing further processing.
  - Multiple streams are transmitting, exacerbating the issue.
- **Impact:** This can lead to significant service disruptions, especially for high-availability systems.

Affected version	Fixed version
HAProxy 3.0	3.0.4
HAProxy 2.9	2.9.10
HAProxy Enterprise 2.9r1	hapee-2.9r1-lb 1.0.0-328.475
HAProxy ALOHA 16.0	16.0.4
HAProxy Kubernetes Ingress Controller 3.0	3.0.1
HAProxy Kubernetes Ingress Controller 1.11	1.11.6
HAProxy Enterprise Kubernetes Ingress Controller 1.11	1.11.6-ee7
HAProxy Enterprise Kubernetes Ingress Controller 1.7	1.7.12-ee12

Workaround: If an immediate update isn't feasible, disable zero-copy forwarding by adding the following line to the global section of the HAProxy configuration:

```
global
    ...
    tune.h2.zero-copy-fwd-send off
```

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

- Regularly monitor HAProxy instances and related network activities for any signs of exploitation.

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.

REFERENCES:

- https://www.haproxy.com/blog/cve-2024-45506