Remote code execution and sensitive secrets exposed through web hook

Critical **aHenryJard** published **GHSA-mf88-g2wq-p7qm** yesterday

Package	Affected versions	Patched versions
No package listed	6.4.8	6.4.11

Description

Summary

Any user with the capability `manage customizations` :

- can execute commands on the underlying infrastructure where OpenCTI is hosted.
- can access internal server side secrets by misusing the web-hooks.

Details

The web-hook feature in OpenCTI allows users to customise messages sent through web-hooks. Provided with a default installation are examples of Microsoft Teams web-hooks. The dynamics of the web-hook is built upon javascript, which a user can enter in a web-hook template field. A malicious user can abuse this to execute commands in the hosting environment on which OpenCTI is executing. A protection layer has been added to guard against using external modules in the javascript code for the web hooks, but these can be bypassed.

A common implementation of OpenCTI is to host it in containers, either directly in docker or in a Kubernetes cluster and in these setups sensitive secrets are passed to the container via environment variables. These environment variables are accessible from the web-hook javascript.

Impact

Since the malicious user gets a root shell inside a container this opens up the the infrastructure environment for further attacks and exposures.

Severity

Critical 9.1 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	High
User interaction	None
Scope	Changed
Confidentiality	High
Integrity	High
Availability	High

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

CVE ID

CVE-2025-24977

Weaknesses

CWE-94

Credits

 **itlabbet** Reporter