Priviledge escalation and unauthenticated access using default admin

Critical **aHenryJard** published **GHSA-6vvv-vmfr-xhrx** yesterday

Package

OpenCTI

Affected versions

>= 6.6.0, < 6.9.13

Patched versions

>= 6.9.13

Description

Impact

There is a priviledge escalation vulnerability affecting OpenCTI that can be exploited by unauthenticated attackers, and enables to query the API as any existing user including the admin set by default.

Patches

This issue has been fixed since version 6.9.13.

Workarounds

There is no workaround for the priviledge escalation issue. One recommended remediation is to disable the default admin using APP__ADMIN__EXTERNALLY_MANAGED configuration.

Severity

Critical 9.8 / 10

CVSS v3 base metrics

Attack vector Network

Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High

Learn more about base metrics

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

CVE ID

CVE-2026-27960

Weaknesses

No CWEs

Credits

 **SouadHadjiat** Reporter