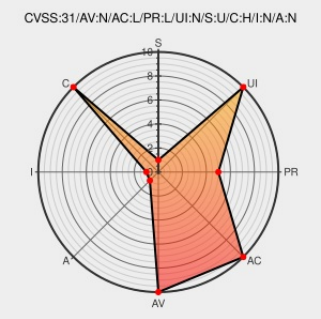
CVE-2020-10100

Published on: 03/04/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-10100

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Zammad from Zammad contain the following vulnerability:

An issue was discovered in Zammad 3.0 through 3.2. It allows for users to view ticket customer details associated with specific customers. However, the application does not properly implement access controls related to this functionality. As such, users of one company are able to access ticket data from other companies. Due to the multi-tenant nature of this application, users who can access ticket details from one organization to the next allows for users to exfiltrate potentially sensitive data of other companies.

CVE-2020-10100 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: 4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link

Zammad – Helpdesk & Support Software | Zammad Security Advisory ZAA-2020-05	Patch Vendor Advisory zammad.com image/svg+xml	MISC zammad.com/news/security-advisory-zaa-2020-05

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Zammad	Zammad	All	All	All	All

cpe:2.3:a:zammad:zammad:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→