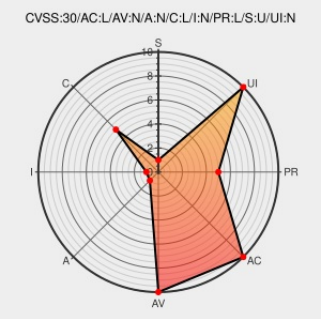
CVE-2019-13457

Published on: 03/10/2020 12:00:00 AM UTC

Last Modified on: 01/27/2023 03:17:00 PM UTC

CVE-2019-13457

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



Certain versions of Otrs from Otrs contain the following vulnerability:

An issue was discovered in Open Ticket Request System (OTRS) 7.0.x through 7.0.8. A customer user can use the search results to disclose information from their "company" tickets (with the same CustomerID), even when the CustomerDisableCompanyTicketAccess setting is turned on.

CVE-2019-13457 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 4.3 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	LOW	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
[security-announce] openSUSE-SU-2020:1475-1: moderate: Recommended updat	lists.opensuse.org text/html	SUSE openSUSE-SU-2020:1475
[security-announce] openSUSE-SU-2020:0551-1: moderate: Recommended updat	lists.opensuse.org text/html	SUSE openSUSE-SU-2020:0551

Release and Security Notes Archive | community.otrs.com	Vendor Advisory www.otrs.com text/html	MISC www.otrs.com/category/release-and-security-notes-en/
[security-announce] openSUSE-SU-2020:1509-1: moderate: Recommended updat	lists.opensuse.org text/html	SUSE openSUSE-SU-2020:1509
OTRS Security Advisory 2019-11 | OTRS	Vendor Advisory otrs.com text/html	CONFIRM otrs.com/release-notes/otrs-security-advisory-2019-11/

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:otrs:otrs:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→