SSRF protection bypass via broken CIDR check in checkIpByMask()

High **freescout-help-desk** published **GHSA-c9v3-4c59-x5q2** 5 days ago

Package

php **freescout-helpdesk/freescout** (Composer)

Affected versions	Patched versions
< 1.8.211	1.8.211

Description

Summary

`checkIpByMask()` in `app/Misc/Helper.php` (line 1967) checks whether the input IP contains a `/` character. Plain IP addresses never contain `/`, so the function always returns false without checking any CIDR ranges. The entire 10.0.0.0/8 and 172.16.0.0/12 private ranges are unprotected.

Root Cause

`app/Misc/Helper.php` lines 1965-1979:

```
public static function checkIpByMask($ip, $masks = [])
{
    if (!strstr($ip, '/')) {   // BUG: checks $ip instead of $mask
        return false;           // Plain IPs never contain '/' -> always returns false
    }
    foreach ($masks as $mask) {
        if (!strstr($mask, '/')) {
            continue;
        }
        if (\Symfony\Component\HttpFoundation\IpUtils::checkIp($ip, $mask)) {
            return $mask;
        }
    }
```

```
    return false;
}
```

The `strstr($ip, '/')` check on line 1967 should not be there. The loop already handles non-CIDR entries with `strstr($mask, '/')` on line 1971. The Symfony `IpUtils::checkIp()` call on line 1974 is dead code.

This was introduced in commit `1e319c91e` ("Improve Helper::sanitizeRemoteUrl() function", 2026-03-07) which added the CIDR ranges and this function.

Bypassed Ranges

These CIDR entries in `restricted_hosts` (line 1887-1903) are never enforced:

- `10.0.0.0/8` (entire RFC1918 Class A)
- `172.16.0.0/12` (entire RFC1918 Class B)
- `fd00::/8` (IPv6 ULA)

Also missing from the list entirely: `192.168.0.0/16`.

Exact-match entries like `127.0.0.1`, `0.0.0.0`, `169.254.169.254`, `localhost` still work via `in_array()`.

Attack Path

FreeScout processes inbound emails with remote attachment URLs via `downloadRemoteFileAsTmp()`, which calls `sanitizeRemoteUrl()` then `checkUrlIpAndHost()`. An email containing an attachment URL pointing to `http://10.0.0.1/internal-api` bypasses the CIDR check and is fetched by the server.

Suggested Fix

Remove the early return on line 1967:

```
public static function checkIpByMask($ip, $masks = [])
{
    foreach ($masks as $mask) {
        if (!strstr($mask, '/')) {
            continue;
        }
        if (\Symfony\Component\HttpFoundation\IpUtils::checkIp($ip, $mask)) {
            return $mask;
        }
    }
    return false;
}
```

Also add `192.168.0.0/16` to `restricted_hosts`.

Severity

High

CVE ID

CVE-2026-34443

Weaknesses

▶ CWE-918

Credits

kodareef5 Reporter