SSRF via 0.0.0.0 bypass in activitypub-federation-rust v4_is_invalid()

Moderate **Nutomic** published **GHSA-q537-8fr5-cw35** 2 weeks ago

Package

activitypub_federation (Rust)

Affected versions	Patched versions
<= 0.7.1	None

Description

Summary

The `v4_is_invalid()` function in `activitypub-federation-rust` (`src/utils.rs`) does not check for `Ipv4Addr::UNSPECIFIED` (0.0.0.0). An unauthenticated attacker controlling a remote domain can point it to 0.0.0.0, bypass the SSRF protection introduced by the fix for CVE-2025-25194 (GHSA-7723-35v7-qcxw), and reach localhost services on the target server.

Note: This vulnerability is in the upstream library `activitypub-federation-rust`, not in Lemmy's own code. Filing here because `activitypub-federation-rust` does not have private vulnerability reporting enabled, and the same maintainers manage both repositories.

Details

File: `src/utils.rs` in `activitypub-federation-rust`
Function: `v4_is_invalid(v4: Ipv4Addr) -> bool`

The function checks `is_private()`, `is_loopback()`, `is_link_local()`, `is_multicast()`, and `is_documentation()` — but omits `is_unspecified()`. On Linux, macOS, and Windows, TCP connections to 0.0.0.0 are routed to localhost (127.0.0.1).

Additionally, `::ffff:0.0.0.0` (IPv4-mapped IPv6) also bypasses because `v6_is_invalid()` calls `to_ipv4_mapped().is_some_and(v4_is_invalid)`, inheriting the same gap. Notably, `v6_is_invalid()` already includes `is_unspecified()` for native IPv6, making this an asymmetric oversight.

Independent secondary finding — DNS Rebinding TOCTOU:
`is_invalid_ip()` resolves DNS via `lookup_host()` for validation, but `reqwest` resolves DNS again for the actual connection. With TTL=0 DNS responses, an attacker can return a legitimate IP for the first resolution (passes check) and 127.0.0.1 for the second (reqwest connects to localhost). CVSS for rebinding alone: 4.8 (AC:H).

PoC

1. Logic Proof (reproduced from source):

```
fn v4_is_invalid(v4: Ipv4Addr) -> bool {
    v4.is_private()
        || v4.is_loopback()
        || v4.is_link_local()
        || v4.is_multicast()
        || v4.is_documentation()
    // BUG: Missing || v4.is_unspecified()
}

assert_eq!(v4_is_invalid(Ipv4Addr::UNSPECIFIED), false);  // 0.0.0.0 PASSES validation
assert_eq!(v4_is_invalid(Ipv4Addr::LOCALHOST), true);     // 127.0.0.1 correctly blocked
```

2. OS Routing Verification:

```
$ connect(0.0.0.0:80) → ConnectionRefused
```

ConnectionRefused proves the OS routed to localhost (port 80 not listening). Any service on 0.0.0.0:PORT is reachable.

3. Attack Chain:

1. Attacker configures DNS: `evil.com A → 0.0.0.0`
2. ii. Attacker sends ActivityPub activity referencing `https://evil.com/actor`
3. iii. Library calls `verify_url_valid()` → `is_invalid_ip()` → resolves to 0.0.0.0
4. iv. `v4_is_invalid(0.0.0.0)` returns `false` (BYPASS)
5. v. `reqwest` connects to 0.0.0.0 → reaches localhost services

Impact

- **Direct:** Bypasses the SSRF protection layer for all ActivityPub federation traffic
- - **Downstream:** 6+ dependent projects affected including Lemmy (13.7k stars), hatsu, gill, ties, fediscus, fediverse-axum
- - **Attacker can:** Access cloud instance metadata (169.254.169.254 via rebinding), reach internal services on localhost, port scan internal infrastructure

Suggested Fix

```rust
fn v4_is_invalid(v4: Ipv4Addr) -> bool {
    v4.is_private()
        || v4.is_loopback()
        || v4.is_link_local()
        || v4.is_multicast()
        || v4.is_documentation()
        || v4.is_unspecified()    // ADD: blocks 0.0.0.0
        || v4.is_broadcast()      // ADD: blocks 255.255.255.255
}
```

For DNS rebinding TOCTOU, pin the resolved IP:

```rust
let resolved_ip = lookup_host((domain, 80)).await?;
// validate resolved_ip...
let client = reqwest::Client::builder()
    .resolve(domain, resolved_ip)  // pin resolution
    .build()?;
```

Severity

Moderate 6.5 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2026-33693

Weaknesses

▶ CWE-918

Credits

SnailSploit Reporter