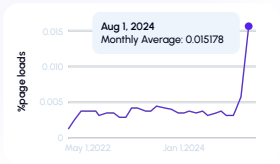
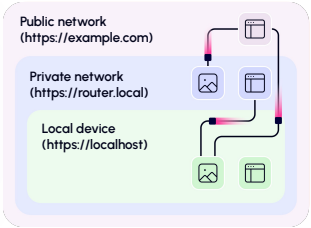
0.0.0.0 Day: Exploiting Localhost APIs From The Browser

01 0.0.0.0: The Unexpected Gateway to Your Internal Network

A vulnerability allows attackers to exploit the 0.0.0.0 IP address to access internal resources (such as developer code or internal messages) through your browser.

0.0.0.0 Day: What It Looks Like





02 Bypassing Security (Private Network Access)

Malicious websites can use JavaScript to send requests to 0.0.0.0, tricking browsers into granting access to private APIs and services.

Bypassing PNA

With PNA, "more private domain" are blocked

- ✗ Localhost
- ✗ 127.0.0.1
- ✗ Hosts file records
- ✗ 192.168.X.X
- ✗ 10.10.X.X

But not when using 0.0.0.0!

- ✓ Localhost
- ✓ 127.0.0.1
- ✓ Hosts file records

03 Who's Vulnerable?

This vulnerability affects both individuals and organizations, potentially compromising sensitive data and applications.

Everything HTTP

- ✓ Port-Forwarding to http services (developers)
- ✓ Operating System services
- ✓ Internal Network Access
  - ✓ VPN access to internal DNS records
  - ✓ DNS Rebinding

04 Browser Fixes

All major browsers have fixed the vulnerability, both by blocking access to 0.0.0.0 explicitly and also by changing the fetch specification.

- **Chromium blocked** 0.0.0.0
- **Safari (WebKit) blocked** 0.0.0.0
- **Fetch (Standard) blocks** 0.0.0.0

Read the full blog

oligo

Mic McCully
Field CTO

05 Example Attack Flow

A The victim runs HTTP service on **localhost**

B Victim visits the **attacker website**

C Attacker Javascript invokes HTTP POST **0.0.0.0 as target IP** & reaches the service