# ProxyAgent vulnerable to MITM

High **mcollina** published **GHSA-pgw7-wx7w-2w33** on Jun 13

Package

undici (npm)

Affected versions

>= v4.8.2 <= 5.5.0

Patched versions

>= v5.5.1

Description

## Description

`Undici.ProxyAgent` never verifies the remote server's certificate, and always exposes all request & response data to the proxy. This unexpectedly means that proxies can MitM all HTTPS traffic, and if the proxy's URL is HTTP then it also means that nominally HTTPS requests are actually sent via plain-text HTTP between Undici and the proxy server.

## Impact

This affects all use of HTTPS via HTTP proxy using **`Undici.ProxyAgent`** with Undici or Node's global `fetch`. In this case, it removes all HTTPS security from all requests sent using Undici's `ProxyAgent`, allowing trivial MitM attacks by anybody on the network path between the client and the target server (local network users, your ISP, the proxy, the target server's ISP, etc).
This less seriously affects HTTPS via HTTPS proxies. When you send HTTPS via a proxy to a remote server, the proxy can freely view or modify all HTTPS traffic unexpectedly (but only the proxy).

Example:

```
setGlobalDispatcher(new ProxyAgent('http://localhost:8000/')) // HTTP Proxy
// or
undici.request('https://example.com/', { dispatcher: new ProxyAgent('http://localhost:8000') })
// or
fetch('https://example.com/', { dispatcher: new ProxyAgent('http://localhost:8000') }) // HTTP P
```

## Patches

This issue was patched in Undici v5.5.1.

## Workarounds

At the time of writing, the only workaround is to not use `ProxyAgent` as a dispatcher for TLS Connections.

## For more information

If you have any questions or comments about this advisory:

- Open an issue in undici repository
- To make a report, follow the SECURITY document

**Severity**

High 7.7 / 10

**CVSS base metrics**

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

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

**CVE ID**

CVE-2022-32210

**Weaknesses**

CWE-295

**Credits**

pimterry