oauthlib / **oauthlib** Public

<> Code ⊙ Issues 72 Pull requests 11 ▷ Actions **Security** 1 Insights

DoS when attacker provide malicious IPV6 URI

Moderate **JonathanHuot** published **GHSA-3pgj-pg6c-r5p7** on Sep 9

Package

oauthlib (pip)

Affected versions	Patched versions
>=3.1.1	3.2.2

Description

Impact

- Attacker providing malicious redirect uri can cause DoS to oauthlib's web application.
- Attacker can also leverage usage of `uri_validate` functions depending where it is used.

What kind of vulnerability is it? Who is impacted?
Oauthlib applications using OAuth2.0 provider support or use directly `uri_validate` function.

Patches

Has the problem been patched? What versions should users upgrade to?
Issue fixed in 3.2.1 release.

Workarounds

Is there a way for users to fix or remediate the vulnerability without upgrading?
The `redirect_uri` can be verified in web toolkit (i.e `bottle-oauthlib` , `django-oauth-toolkit` , ...) before oauthlib is called. A sample check if `:` is present to reject the request can prevent the DoS, assuming no port or IPv6 is fundamentally required.

References

Attack Vector:

- Attacker providing malicious redirect uri:

  oauthlib/oauthlib/oauth2/rfc6749/grant_types/base.py
  Line 232 in d4bafd9

  ```
  232       if not is_absolute_uri(request.redirect_uri):
  ```

- Vulnerable `uri_validate` functions: https://github.com/oauthlib/oauthlib/blob/2b8a44855a51ad5a5b0c348a08c2564a2e197ea2/oauthlib/uri_validate.py

PoC

```
is_absolute_uri("http://[:::::::::::::::::::::::::::::::::::::::]/path")
```

Acknowledgement

Special thanks to Sebastian Chnelik - PyUp.io

Severity

Moderate 5.7 / 10

CVSS base metrics

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

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

CVE ID

CVE-2022-36087

Weaknesses

No CWEs

Credits

SCH227