Vulnerability allows attacker to fake their email address during authentication

Moderate **nhosoya** published **GHSA-49r3-2549-3633** on Dec 2, 2020

Package

omniauth-apple (RubyGems)

Affected versions	Patched versions
<=1.0.0	1.0.1

Description

Impact

This vulnerability impacts applications using the omniauth-apple strategy of OmniAuth and using the `info.email` field of OmniAuth's Auth Hash Schema for any kind of identification. The value of this field may be set to any value of the attacker's choice including email addresses of other users.

For example, an application using omniauth-apple with the following code will be impacted:

```
def omniauth_callback
    auth_hash = request.env['omniauth.auth']
    @authenticated_user = User.find_by(email: auth_hash.info.email)
end
```

Applications not using `info.email` for identification but are instead using the `uid` field are not impacted in the same manner. Note, these applications may still be negatively affected if the value of `info.email` is being used for other purposes.

Patches

Applications using affected versions of omniauth-apple are advised to upgrade to omniauth-apple version 1.0.1 or later.

Workarounds

If unable to upgrade to a patched version, monkey patching `OmniAuth::Strategies::Apple#email` as follows is advised as a workaround:

```
module OmniAuth
  module Strategies
    class Apple
      def email
        id_info['email']
      end
    end
  end
end
```

References

Commit with fix: `b37d540`
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26254

Severity

Moderate

CVE ID

CVE-2020-26254

Weaknesses

No CWEs

Credits

davidtaylorhq