**Problem**

<https://github.com/juliangruber/keypair/security/advisories/GHSA-3f99-hvg4-qjwj>

**index.js**

var crypto = null;

b.putByte(String.fromCharCode(next & 0xFF)); **(C’est vraiment cette ligne qui cause problème).**

The definition of putByte is

util.ByteBuffer.prototype.putByte = function(b) {

this.data += String.fromCharCode(b);

};

**Conséquence:**

* String.fromCharCode(String.fromCharCode(next & 0xFF))

This results in most of the buffer containing zeros (**approximately 97% of the bytes are converted to zeros**).

* each byte in the RNG seed has a 97% chance of being 0 due to incorrect conversion

**Fix**

**index.js**

var crypto;

try {

crypto = require('crypto');

} catch (\_) {}

* Extra protection: If the crypto module is available, it is used instead of the pseudo-random number generator.

True fix:

b.putByte(next & 0xFF);