Hardcoded-key vulnerability usage of static salt #190

⊙ Open **LennonCMJ** opened this issue on Feb 19, 2019 · 1 comment

LennonCMJ commented on Feb 19, 2019 • edited

Application uses static key when performing encryption which makes it easier for an attacker to conduct brute force password guessing.

```
Affected URL: https://github.com/doramart/DoraCMS/blob/9fee40914eccfd06dc225ebdd3e7c4bff0be799f/server/lib/utils/crypto.js

const AESkey = "doracms_";
const MD5key = "dora";
export default {
        AES: {
                encrypt: (message) => {//加密
                        return CryptoJS.AES.encrypt(message, AESkey, {
                                mode: CryptoJS.mode.CBC,
                                padding: CryptoJS.pad.Pkcs7
                        }).toString();
                },



Affected URL:
https://github.com/doramart/DoraCMS/blob/9fee40914eccfd06dc225ebdd3e7c4bff0be799f/server/lib/controller/user.js

  if (fields.password) {
                userObj.password = service.encrypt(fields.password, settings.encrypt_key);
            }



Solution usage of a random salt :
 this.encrypt = function(message, password) {
        var salt = forge.random.getBytesSync(128);
        var key = forge.pkcs5.pbkdf2(password, salt, 4, 16);
        var iv = forge.random.getBytesSync(16);
        var cipher = forge.cipher.createCipher('AES-CBC', key);
        cipher.start({iv: iv});
        cipher.update(forge.util.createBuffer(message));
        cipher.finish();
        var cipherText = forge.util.encode64(cipher.output.getBytes());
        return {cipher_text: cipherText, salt: forge.util.encode64(salt), iv: forge.util.encode64(iv)};
    }
```

Source
https://auth0.com/blog/adding-salt-to-hashing-a-better-way-to-store-passwords/
https://www.thepolyglotdeveloper.com/2014/10/implement-aes-strength-encryption-javascript/
https://cwe.mitre.org/data/definitions/329.html

doramart commented on Feb 22, 2019 Owner

Thank you, I will confirm that

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

2 participants