Potential secrets being logged to disk (2)

High slubar published GHSA-mpwm-rmqp-7629 on May 25

Package

data.js (CVE Services)

Affected versions

cve service >1.1.1

Patched versions

None

Description

Description

In the conditional below, there seems to be a potential for production secrets to be written to disk:(

cve-services/src/utils/data.js
Lines 68 to 83 in 6b085e4

```
68      if (process.env.NODE_ENV === 'development') {
69        user.secret = hash
70      } else {
71        const randomKey = cryptoRandomString({ length: CONSTANTS.CRYPTO_RANDOM_STRING_L
72        user.secret = await argon2.hash(randomKey)
73
74        // write each user's API key to file
75        // necessary when standing up any new shared instance of the system
76        const payload = { username: user.username, secret: randomKey }
77        fs.writeFile(apiKeyFile, JSON.stringify(payload) + '\n', { flag: 'a' }, (err) =
```

)

This method writes the generated randomKey to disk with lines 76 and 77 if the environment is not development.

If this method were called in production, would it not write that plaintext key to disk?

Notes:

Any modifications/remediation must be implemented in Master Branch as a "hot fix" to CVE Service 1.1.1 in production as well as in the Dev Branch so that the changes make their way into CVE Services 2.x

Severity

High

CVE ID

CVE-2022-31004

Weaknesses

CWE-779