「漏洞通告」

SonarQube api 信息泄露漏洞安全风险通告

近几日，某安全厂商监测到有境外恶意攻击者利用一款名为 SonarQube 的代码质量管理系统的漏洞攻击受害者并窃取其项目源代码的行为。漏洞为 2020 年出现的 SonarQube api 信息泄露漏洞，鉴于漏洞高危，构成软件供应链安全风险，请各自全面排查是否采用此系统做软件质量管理，是否因默认配置而受漏洞影响，以免发生源代码等项目资产被窃取的安全事件。

漏洞描述

SonarQube 是一个开源的代码分析平台，可以用来持续分析和评测项目源代码的质量。此平台某接口存在信息泄露漏洞，可以获取部分敏感信息。

漏洞编号

CVE-2020-27986

漏洞等级

高危

受影响版本

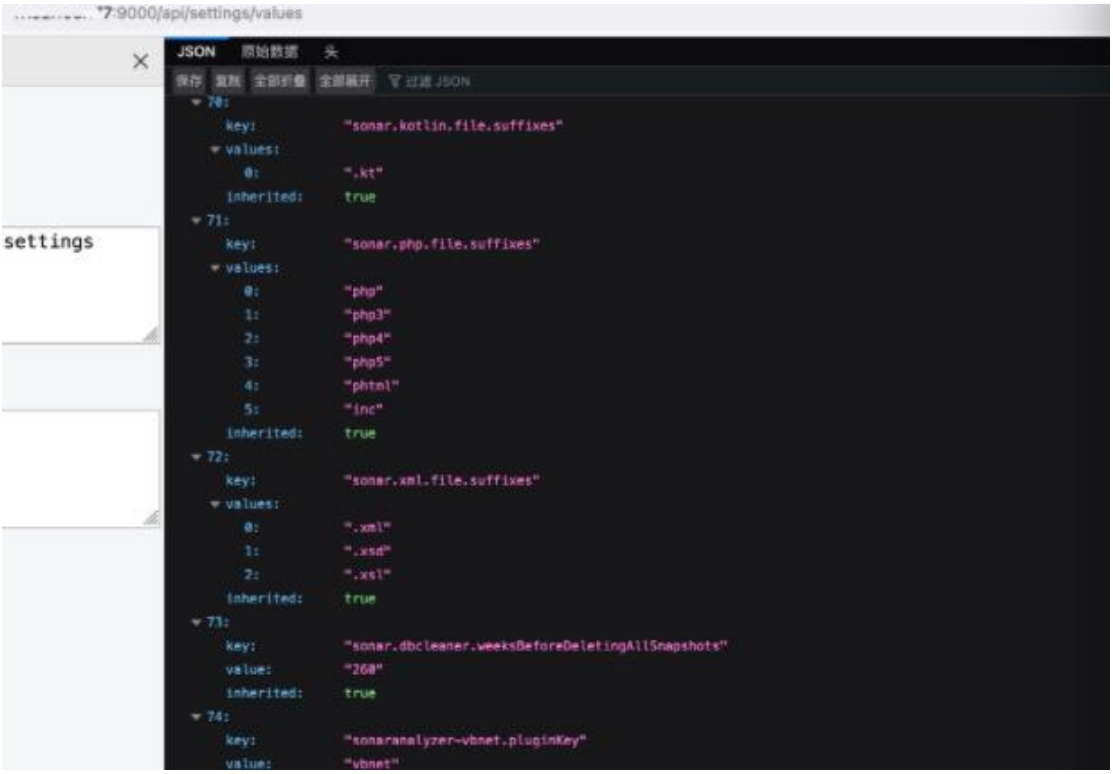
SonarQube

漏洞自查

Fofa 查询语句：app="sonarQube-代码管理"

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

可泄露的为：明文 SMTP、SVN 和 Gitlab 等敏感信息



处置措施

1、暂时下线暴漏在互联网上的 SonarQube。
2、修改源码中硬编码的数据库账户密码、密钥、api 接口等信息。

额外通知

SnoarQube系统存在未授权访问漏洞

★ 关注(0)

CNVD-ID	CNVD-2021-84502
公开日期	2021-11-05
危害级别	高 (AV:N/AC:L/Au:N/C:C/I:N/A:N)
影响产品	SnoarQube SnoarQube开源版 <= 9.1.0.47736 SnoarQube SnoarQube稳定版 <= 8.9.3
漏洞描述	SnoarQube是一个管理代码质量的开源平台，可以集成不同的测试工具、代码分析工具以及持续集成工具。通过不同的插件对分析结果进行再加工处理，通过量化的方式度量代码质量的变化，从而可以方便地对不同规模和种类的工程进行代码质量的管理。 SnoarQube系统存在未授权访问漏洞，该是由于SnoarQube系统配置不当，导致平台项目暴露在公网当中，攻击者利用该漏洞访问公网API接口，使用系统默认配置口令进入平台，下载源代码文件，获取系统敏感信息。
漏洞类型	通用型漏洞
参考链接	https://docs.sonarqube.org/latest/setup/get-started-2-minutes/
漏洞解决方案	目前没有详细解决方案提供： https://www.sonarqube.org/downloads/
厂商补丁	(无补丁信息)
验证信息	(暂无验证信息)
报送时间	2021-11-05
收录时间	2021-11-05

cnvd 最近公开了一个 SnoarQube 系统存在未授权访问攻击的漏洞，官方暂未提供解决方案，请持续关注官方消息。