YApi mongo 注入漏洞通告

■ 通告编号 NS-2022-00	■ 发布日期 2022-11-11
■ 危害等级	攻击者利用此漏洞，可实现 token 泄露、远程代码执行
■ TAG	YApi、mongo、token 泄露、远程代码执行

一. 漏洞概述

近日，绿盟科技 CERT 监测到网上公开发布了一个开源 API 接口管理平台 YApi mongo 注入漏洞，由于 YApi 中某函数存在拼接，能够实现 MongoDB 注入，未经身份验证的远程攻击者可通过利用该漏洞获取到用户 token（包括用户 ID、项目 ID 等必要参数）。同时，可结合自动化测试 API 接口写入待执行命令，并利用沙箱逃逸，最终导致命令执行。目前官方已发布安全补丁修复该漏洞，请受影响的用户尽快采取措施进行防护。

YApi 是一款高效、易用、功能强大的开源 api 管理平台，能够为开发、产品、测试人员提供更优雅的接口管理服务，开发人员只需利用平台提供的接口数据写入工具以及简单的点击操作就可以实现接口的管理。

参考链接：

https://github.com/YMFE/yapi/commit/59bade3a8a43e7db077d38a4b0c7c584f30ddf8c?diff=split

二. 影响范围

受影响版本

- YApi < 1.12.0

不受影响版本

- YApi >= 1.12.0

注：在默认配置下不受漏洞影响

三. 漏洞防护

3.1 官方升级

目前官方已发布安全版本修复此漏洞，建议受影响的用户及时升级防护：https://github.com/YMFE/yapi/releases/tag/v1.12.0

补丁链接：https://github.com/YMFE/yapi/commit/59bade3a8a43e7db077d38a4b0c7c584f30ddf8c

3.2 临时防护措施

在不影响业务的情况下，可对 YAPI 平台的访问进行限制。

声明