Harbor 未授权访问漏洞（CVE-2022-46463）通告

■ 通告编号 **NS-2023-00**	■ 发布日期 **2023-01-16**
■ 漏洞危害	**攻击者利用此漏洞可实现对系统进行未授权访问**
■ **TAG**	Harbor、未授权访问、CVE-2022-46463

一. 漏洞概述

近日，绿盟科技 CERT 监测到网上公开披露了 Harbor 未授权访问漏洞（CVE-2022-46463）的技术细节，由于 Harbor 中存在访问控制缺陷，无需身份验证的攻击者可通过该漏洞访问公共和私有镜像存储库的所有信息，并进行镜像拉取。目前，该漏洞技术细节与 PoC 已公开，请受影响的用户尽快采取措施进行防护。

Harbor 是一个开放源代码可信云本机注册表项目，用于存储，签名和扫描内容。Harbor 通过添加用户通常需要的功能（例如安全性，身份和管理）扩展了开源 Docker Distribution。使注册表更接近于构建和运行环境可以提高图像传输效率。

参考链接：

https://github.com/advisories/GHSA-5c53-mg2q-8qhc

二. 影响范围

受影响版本

- v1.x <= Harbor <= v2.5.3

不受影响版本

- Harbor v2.5.x > v2.5.3
- Harbor v2.6.x
- Harbor v2.7.x

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/goharbor/harbor/releases

声明

本安全公告仅用来描述可能存在的安全问题，绿盟科技不为此安全公告提供任何保证或承诺。由于传播、利用此安全公告所提供的信息而造成的任何直接或者间接的后果及损失，均由使用者本人负责，绿盟科技以及安全公告作者不为此承担任何责任。

绿盟科技拥有对此安全公告的修改和解释权。如欲转载或传播此安全公告，必须保证此安全公告的完整性，包括版权声明等全部内容。未经绿盟科技允许，不得任意修改或者增减此安全公告内容，不得以任何方式将其用于商业目的。