



# 网络安全预警通报

(总第 24 期)

长江大学互联网与信息中心 2023 年 5 月 24 日

【预警类型】 高危预警

【预警内容】 关于 Joomla 存在未授权访问漏洞的安全公告

安全公告编号: CNTA-2023-0005

国家信息安全漏洞共享平台 (CNVD) 收录了 Joomla 未授权访问漏洞 (CNVD-2023-11024, 对应 CVE-2023-23752)。未经授权的攻击者可远程利用该漏洞获得服务器敏感信息。目前, 该漏洞的利用细节和测试代码已公开, 厂商已发布新版本完成修复。CNVD 建议受影响的单位和用户立即升级到最新版本。

## 一、漏洞概述

Joomla 是由 Open Source Matters 开源组织研发和维护的知名内容管理系统 (CMS), 它使用 PHP 语言和 MySQL 数据库开发, 兼容 Linux、Windows、MacOSX 等多种系统平台。近日, Joomla 官方发布安全公告, 修复了 Joomla 未授权访问漏洞。由于 Joomla 对 Web 服务端点缺乏必要的访问限制, 未经身份认证的攻击者, 可以远程利用此漏洞访问服务器 REST API 接口, 造成服务器敏感信息泄露。

## 二、漏洞影响范围

漏洞影响的产品和版本: 4.0.0 <= Joomla <= 4.2.7

## 三、漏洞处置建议

目前，Joomla 官方已发布新版本修复该漏洞，CNVD 建议受影响的单位和用户立即升级至 4.2.8 及以上版本：

<https://downloads.joomla.org/>

<https://github.com/joomla/joomla-cms/releases/tag/4.2.8>

参考链接

[https://mp.weixin.qq.com/s/W9SWcP6Ikv\\_0KRTDD3y9b](https://mp.weixin.qq.com/s/W9SWcP6Ikv_0KRTDD3y9b)