



مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



**Exploited Critical Vulnerability in Marimo**  
Tracking #:432318769  
Date:12-04-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical remote code execution (RCE) vulnerability, CVE-2026-39987, affecting the open-source Python notebook platform Marimo.

## TECHNICAL DETAILS:

A critical remote code execution (RCE) vulnerability, CVE-2026-39987, affecting the open-source Python notebook platform Marimo, has been actively exploited within 10 hours of public disclosure. The flaw enables unauthenticated attackers to gain full system-level access via a misconfigured WebSocket endpoint. Observations confirm real-world exploitation involving manual reconnaissance and credential harvesting, underscoring the accelerating threat window between vulnerability disclosure and exploitation.

Organizations using Marimo in internet-facing environments face immediate risk of compromise, particularly where sensitive data (e.g., .env files, SSH keys) is present.

### Vulnerability Overview

- CVE ID: CVE-2026-39987
- CVSS Score: 9.3 (**Critical**)
- Affected Software: Marimo  $\leq$  v0.20.4
- Patched Version: v0.23.0
- Vulnerability Type: Pre-authentication Remote Code Execution (RCE)
- Attack Vector: Network (WebSocket endpoint exposure)
- Authentication Required: None

## RECOMMENDATIONS:

### Immediate Actions:

- Upgrade Marimo immediately to fixed version.
- Disable external access to Marimo instances until patched.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

## REFERENCES:

- <https://github.com/marimo-team/marimo/security/advisories/GHSA-2679-6mx9-h9xc>