Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

From Advisory to Attack in Under 10 Hours: Marimo's Critical RCE Flaw

Date of Publication	Admiralty Code	TA Number
April 14, 2026	A1	TA2026100

Summary

First Seen: April 8, 2026
Affected Products: Marimo (versions prior to 0.23.0)
Impact: CVE-2026-39987 is a critical pre-authenticated remote code execution vulnerability in Marimo, an open-source Python notebook platform, affecting all versions prior to 0.23.0. The flaw stems from the /terminal/ws WebSocket endpoint lacking authentication checks, allowing unauthenticated attackers to obtain a full interactive shell and execute arbitrary commands. Active exploitation within just 9 hours and 41 minutes of the advisory's publication on April 8, 2026, with attackers crafting working exploits directly from the advisory, no public PoC required. Organizations are urged to upgrade to version 0.23.0 immediately, rotate any exposed credentials, and implement additional network-layer authentication controls.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-39987	Marimo Terminal WebSocket Pre-Auth Remote Code Execution Vulnerability	Marimo-Team Marimo	✗	✓	✓

Vulnerability Details

#1 CVE-2026-39987 is a critical pre-authenticated remote code execution vulnerability (CVSS 9.3) affecting Marimo, an open-source reactive Python notebook platform used for data science, analysis, and interactive coding. The flaw impacts all versions prior to 0.23.0

#2 The root cause lies in the /terminal/ws WebSocket endpoint, which completely skips authentication validation, unlike other endpoints such as /ws that properly invoke the validate_auth() function. This allows any unauthenticated attacker to obtain a full PTY shell and execute arbitrary system commands through a single WebSocket connection.

#3 The vulnerability was publicly disclosed on April 8, 2026, and exploitation in the wild was observed by researchers within just 9 hours and 41 minutes, with no public proof-of-concept code available at the time. The attacker crafted a working exploit directly from the advisory description, connected to the unauthenticated terminal endpoint on a honeypot, and conducted manual reconnaissance over four sessions spanning 90 minutes.

#4 Activities focused on harvesting credentials from .env files, searching for SSH keys, and exploring the file system. No malware, cryptominers, or backdoors were deployed; the objective was purely credential theft and data harvesting for potential later use or resale.

#5 The impact extends beyond simple server compromise. Marimo environments frequently store sensitive API keys for LLM providers and cloud services, meaning exfiltrated credentials could enable lateral movement into cloud infrastructure, abuse of AI services, and exposure of training datasets or model artifacts.

#6 Organizations running Marimo should upgrade to version 0.23.0 immediately, rotate all exposed credentials, audit access logs for unauthorized WebSocket connections to /terminal/ws, and implement reverse-proxy-based authentication as an additional defense layer. This incident highlights the rapidly shrinking window between vulnerability disclosure and active exploitation.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-39987	Marimo versions before 0.23.0	cpe:2.3:a:marimo-team:marimo:*:*:*:*:*:python:*:*	CWE-306

Recommendations

Upgrade Marimo Immediately: Update all Marimo instances to version 0.23.0 or later without delay. This release addresses the authentication bypass on the terminal WebSocket endpoint by aligning it with the validation logic used by other WebSocket routes. If upgrading is not immediately feasible, restrict network access to the `/terminal/ws` endpoint or disable the terminal feature entirely until the patch can be applied.

Audit and Rotate Exposed Credentials: For any Marimo instance that has been publicly accessible or reachable from untrusted networks, immediately audit environment variables, `.env` files, and stored secrets on the host. Rotate all potentially exposed credentials including AWS access keys, API tokens, database passwords, and SSH keys as a precautionary measure, even if no confirmed breach has been identified.

Restrict Network Exposure of Notebook Environments: Do not expose Marimo edit mode to untrusted networks. Deploy instances behind VPNs, private subnets, or authenticated reverse proxies with strict allowlists. Avoid binding the server to 0.0.0.0 unless network-level controls are explicit and verified. Notebook platforms should never be directly accessible from the public internet without an additional authentication layer.

Harden Container Deployments: Where Marimo is deployed in containerized environments, ensure that the process runs as a non-root user, use read-only root filesystems where practical, and apply minimal Linux capabilities. While container hardening does not prevent pre-authentication RCE, it significantly limits the blast radius of a successful compromise.

Implement WebSocket Monitoring and Detection: Monitor for WebSocket connections to the `/terminal/ws` path from unexpected sources. Alert on new shell processes, unusual process trees, and anomalous egress traffic from notebook infrastructure. Legitimate terminal usage should be restricted to authenticated users on internal networks only.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	T1059.004: Unix Shell
		T1059.006: Python
Discovery	T1083: File and Directory Discovery	
	T1016: System Network Configuration Discovery	
	T1082: System Information Discovery	
Credential Access	T1552: Unsecured Credentials	T1552.001: Credentials In Files
Collection	T1005: Data from Local System	
Lateral Movement	T1021: Remote Services	T1021.004: SSH

Patch Link

https://github.com/marimo-team/marimo/releases

References

https://webflow.sysdig.com/blog/marimo-oss-python-notebook-rce-from-disclosure-to-exploitation-in-under-10-hours

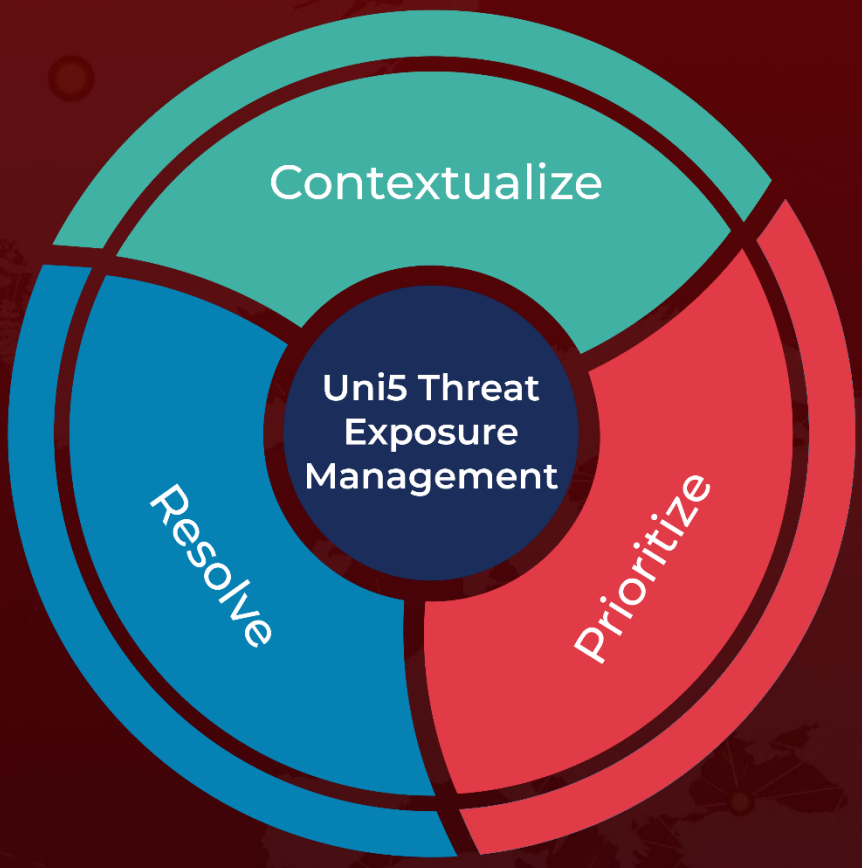
https://github.com/advisories/GHSA-2679-6MX9-H9XC

https://labs.cloudsecurityalliance.org/research/csa-research-note-marimo-rce-cve-2026-39987-ai-toolchain-202/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

April 14, 2026 • 10:30 AM

More at www.hivepro.com