



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Critical OS Command Injection Vulnerability in OneUptime Probe
Tracking #:432318494
Date:02-03-2026

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 vulnerability, CVE-2026-27728 has been identified in the NetworkPathMonitor component of OneUptime Probe.

TECHNICAL DETAILS:

A critical vulnerability, CVE-2026-27728 (CVSS v3.1: 10.0 – Critical), has been identified in the NetworkPathMonitor component of OneUptime Probe. The flaw allows authenticated remote attackers to perform Operating System (OS) Command Injection (CWE-78), leading to Remote Code Execution (RCE) on the underlying server.

Vulnerability Details

- CVE ID: CVE-2026-27728
- CVSS Score: 10.0 (**Critical**)
- CWE Classification: CWE-78 – Improper Neutralization of Special Elements used in an OS Command
- Attack Vector: Network
- Privileges Required: Low (Authenticated user)
- User Interaction: None
- Scope: Potential cross-tenant impact in shared environments

Affected Component

- Product: OneUptime Probe
- Module: NetworkPathMonitor
- Affected Versions: ≤ 10.0.6
- Fixed Version: 10.0.7

RECOMMENDATIONS:

Upgrade Immediately

- Update OneUptime version to fixed version or later.
- Validate successful deployment across all probe instances.

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://www.cve.org/CVERecord?id=CVE-2026-27728>