

مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



**High-severity Vulnerability in NVIDIA UFM**  
Tracking #:432316570  
Date:27-11-2024

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed NVIDIA has issued a security advisory regarding a high-severity authentication vulnerability in several of its Unified Fabric Manager (UFM) products.

## TECHNICAL DETAILS:

NVIDIA has issued a security advisory regarding a high-severity authentication vulnerability in several of its Unified Fabric Manager (UFM) products. The flaw, identified in the Ethernet management interface, could allow an attacker to gain unauthorized access and control of affected systems by sending a malformed request.

### Vulnerabilities Details:

- **CVE-2024-0130**
- **Severity:** High (CVSS 8.8)
- **Impact:** A successful exploit of this vulnerability might lead to escalation of privileges, data tampering, denial of service, and information disclosure.

Affected Products	Platform or OS	Affected Versions	Updated Version
UFM Enterprise GA	RHEL 8, RHEL 9, Ubuntu20, Ubuntu22	6.15.x, 6.16.x, 6.17.x	6.18.0-5
UFM Enterprise LTS23	RHEL 7, RHEL 8, RHEL 9, Ubuntu18, Ubuntu20, Ubuntu22	6.15.x LTS prior to 6.15.6-4 LTS	6.15.6-4 LTS
UFM Enterprise Appliance GA	N/A	1.6.x, 1.7.x, 1.8.x	1.9.1-2
UFM Enterprise Appliance LTS23	N/A	1.6.x LTS prior to 1.6.6-1 LTS	1.6.6-1 LTS
UFM SDN Appliance GA	N/A	4.14.x, 4.15.x, 4.16.x	4.17.0.5
UFM SDN Appliance LTS23	N/A	4.14.x LTS prior to 4.14.6.4 LTS	4.14.6.4 LTS
UFM CyberAI GA	N/A	2.6.x, 2.7.x, 2.8.x	2.9.1-2
UFM CyberAI LTS23	N/A	2.6.1-3 LTS	2.6.1-4 LTS

## RECOMMENDATIONS:

Users of the affected UFM products are strongly encouraged to download and install the firmware update immediately.

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://nvidia.custhelp.com/app/answers/detail/a\\_id/5584](https://nvidia.custhelp.com/app/answers/detail/a_id/5584)