



مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



Security Updates - NVIDIA  
Tracking #:432316938  
Date:06-03-2025

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 that NVIDIA has released a security updates for its Hopper HGX 8-GPU High-Performance Computing (HMC) systems, addressing two significant vulnerabilities.

## TECHNICAL DETAILS:

### Vulnerabilities Details:

- CVE-2024-0114 (CVSS 8.1 - High Severity)**
  - Affects: HGX Management Controller (HMC)
  - Impact: Allows a malicious actor with administrative access to the BMC to gain administrator access to the HMC
  - Potential consequences: Code execution, denial of service, privilege escalation, information disclosure, and data tampering
- CVE-2024-0141 (CVSS 6.8 - Medium Severity)**
  - Affects: GPU VBIOS
  - Impact: Allows an attacker with tenant-level GPU access to write to an unsupported registry
  - Potential consequence: Denial of service

### Affected Products:

- NVIDIA Hopper HGX 8-GPU

### Affected Versions:

- HGX-22.10-1-rc67 (1.5.0)
- HGX-22.10-1-rc63 (1.4.0)
- HGX-22.10-1-rc59 (1.3.2)
- HGX-22.10-1-rc57 (1.3.0/1.3.1)

### Fixed Versions:

- Firmware version 1.6.0 and later

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by NVIDIA.

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/5561](https://nvidia.custhelp.com/app/answers/detail/a_id/5561)