مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in HPE Cray XD670 Servers

Tracking #:432316985

Date:18-03-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in the HPE Cray XD670 Server utilizing the AMI BMC Redfish API. This vulnerability allows remote attackers to bypass authentication, potentially gaining unauthorized access to the server's baseboard management controller (BMC) without valid credentials.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-540385**
- CVSS Score: 10.0 Critical
- A critical vulnerability exits in the AMI BMC Redfish API utilized by HPE Cray XD670 servers. This flaw allows for remote authentication bypass, enabling unauthorized access to the Baseboard Management Controller (BMC). An attacker exploiting this vulnerability could gain complete control of the affected server without providing valid credentials.
- Successful exploitation of this vulnerability poses a severe threat, particularly in high-performance computing (HPC) environments where HPE Cray XD670 servers are commonly deployed. Potential impacts include:
    - Complete server compromise
    - Data breaches
    - System disruption and denial of service
    - Malicious activities such as malware deployment and lateral movement

Affected Versions:

- HPE Cray XD670 - Prior to BMC v1.19

Fixed Versions:

- BMC firmware, version 1.19 or later

RECOMMENDATIONS:

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

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://support.hpe.com/hpesc/public/docDisplay?docId=hpesbcr04828en_us&docLocale=en_US