مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Vulnerability in HPE ProLiant DX Servers

Tracking #:432316395

Date:15-10-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in HPE ProLiant DX Servers that could be exploited to gain unauthorized access to affected systems.

TECHNICAL DETAILS:

A high-severity security vulnerability exists in certain HPE ProLiant DX servers utilizing specific Intel processors. This vulnerability, identified as CVE-2024-39283, allows for a local escalation of privilege, potentially enabling unauthorized users to gain elevated access within the system.

Vulnerability Details:

- **CVE-2024-39283**
- **Severity: High**
- The vulnerability arises from insufficient validation of user input in the BIOS firmware, which can be exploited by a local user to execute arbitrary code with elevated privileges.

Affected Systems:

- **HPE ProLiant DX4120 Gen11** - Prior to v2.20_05-27-2024
- **HPE ProLiant DX560 Gen11** - Prior to v2.20_05-27-2024
- **HPE ProLiant DX380 Gen11** - Prior to v2.20_05-27-2024
- **HPE ProLiant DX380a Gen11** - Prior to v2.20_05-27-2024
- **HPE ProLiant DX360 Gen11** - Prior to v2.20_05-27-2024
- **HPE ProLiant DX320 Gen11** - Prior to v2.20_05-27-2024

Fixed Versions:

- BIOS version 2.20_05-27-2024 or later.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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=hpesbhf04720en_us&docLocale=en_US