

مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



**High-Severity Vulnerabilities in HPE ProLiant Servers**

Tracking #:432317621

Date:21-08-2025

## EXECUTIVE SUMMARY:

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

## TECHNICAL DETAILS:

### Vulnerability Details:

#### CVE-2025-22839

- **Severity:** 7.5 (High)
- A potential security vulnerability has been identified in HPE ProLiant DL/ML/XD products with Intel processors. The issue resides in the Intel Out-of-Band Management (OOBM) Services Module, which could be exploited locally to escalate privileges.

#### CVE-2025-22840

- **Severity:** 7.4 (High)
- A potential security vulnerability has been identified in HPE ProLiant DL/ML/XD Gen12 servers using Intel Xeon 6 Scalable Processors. The vulnerability could be locally exploited to escalate privileges under certain conditions.

### Affected Versions:

- HPE ProLiant Compute DL320 Gen12 - Prior to 1.40\_05-22-2025
- HPE ProLiant Compute DL340 Gen12 - Prior to 1.40\_05-22-2025
- HPE ProLiant Compute DL360 Gen12 - Prior to 1.40\_05-22-2025
- HPE ProLiant Compute DL380 Gen12 - Prior to 1.40\_05-22-2025
- HPE ProLiant Compute DL380a Gen12 - Prior to 1.40\_05-22-2025
- HPE ProLiant Compute DL384 Gen12 - Prior to 1.40\_05-22-2025
- HPE ProLiant Compute DL580 Gen12 - Prior to 1.40\_05-22-2025
- HPE ProLiant Compute ML350 Gen12 - Prior to 1.40\_05-22-2025
- HPE ProLiant Compute XD230 - Prior to 1.40\_05-22-2025

**Fixed Version (Firmware):** BIOS v1.40\_05-22-2025 or later.

## RECOMMENDATIONS:

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

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=hpeshbf04934en\\_us&docLocale=en\\_US](https://support.hpe.com/hpesc/public/docDisplay?docId=hpeshbf04934en_us&docLocale=en_US)
- [https://support.hpe.com/hpesc/public/docDisplay?docId=hpeshbf04933en\\_us&docLocale=en\\_US](https://support.hpe.com/hpesc/public/docDisplay?docId=hpeshbf04933en_us&docLocale=en_US)