مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Multiple Vulnerabilities in HPE Private Cloud AI
Tracking #:432317929
Date:04-11-2025

TLP: WHITE

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in HPE Private Cloud AI could allow remote attackers to perform XSS, information disclosure, or SSRF attacks. Successful exploitation may lead to unauthorized access, data exposure, or service disruption.

TECHNICAL DETAILS:

Vulnerability Details
The issues exist in the integrated AI Essentials (AIE) component of HPE Private Cloud AI.

- **CVE-2023-38408:** Remote code execution risk in an integrated component (CVSS 9.8 – Critical)
- **CVE-2024-47875:** Cross-site scripting (XSS) vulnerability (CVSS 6.1 – Medium)
- **CVE-2025-37150:** Information disclosure (CVSS 4.6 – Medium)
- **CVE-2025-37151:** Privilege-related information exposure (CVSS 4.6 – Medium)
- **CVE-2025-37152:** Server-side request forgery (SSRF) (CVSS 6.3 – Medium)
- **CVE-2025-37153:** Improper input validation leading to SSRF (CVSS 6.3 – Medium)
- **CVE-2025-37154:** Data exposure via SSRF (CVSS 6.3 – Medium)

Affected Versions
- HPE Private Cloud AI – Versions prior to 1.7,
- AI Essentials component stack (up to version AIE 1.10.0).

Fixed Versions
- HPE Private Cloud AI AIE 1.10.0 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=hpesbpc04960en_us&docLocale=en_US#hpesbpc04960-rev-1-hpe-private-cloud-ai-multiple-v-0