مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in HPE AutoPass License Server

Tracking #:432318489

Date:02-03-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in HPE AutoPass License Server (APLS) that could be exploited to gain unauthorized access to affected systems.

TECHNICAL DETAILS:

Hewlett Packard Enterprise has identified a potential security vulnerability in HPE AutoPass License Server (APLS) that could allow a remote attacker to bypass authentication controls. Successful exploitation may permit unauthorized access to the affected system.

Vulnerability Details

- **CVE ID:** CVE-2026-23600
- **Impact:** Remote Authentication Bypass
- **CVSS v3.1 Base Score:** 7.3 (High)
- A vulnerability in HPE AutoPass License Server could allow remote exploitation resulting in authentication bypass. An unauthenticated attacker may be able to gain unauthorized access to the system, potentially impacting confidentiality, integrity, and availability.

Affected Products

- HPE AutoPass License Server (APLS) – Versions prior to 9.19

Fixed Version

- HPE AutoPass License Server (APLS) 9.19 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=hpesbgn05003en_us&doccLocale=en_US