مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in HPE Telco Intelligent Assurance

Tracking #:432318971

Date:16-05-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Multiple high-severity vulnerabilities in HPE Telco Intelligent Assurance. These vulnerabilities affect bundled third-party components and could allow remote attackers to cause Denial of Service (DoS) or exploit HTTP Request Smuggling issues, potentially impacting service availability and request integrity.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE-2025-52999 | High | CVSS 7.5**
  A vulnerability may allow unauthenticated remote attackers to trigger a Denial of Service (DoS) condition.
- **CVE-2026-33870 | High | CVSS 7.5**
  A vulnerability may allow HTTP Request Smuggling or inconsistent interpretation of HTTP requests, which could impact request integrity.
- **CVE-2026-33871 | High | CVSS 7.5**
  A vulnerability may allow unauthenticated remote attackers to cause a Denial of Service (DoS) condition.

Affected Versions

- HPE Telco Intelligent Assurance 4.2.14 and earlier

Fixed Version

- HPE Telco Intelligent Assurance FAS & PDO 4.2.15 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=hpesbnw05045en_us&docLocale=en_US