مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Critical Vulnerabilities in HPE Insight Remote Support

Tracking #:432316577

Date:29-11-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Hewlett Packard Enterprise (HPE) has issued an urgent security update for its Insight Remote Support service, addressing multiple critical vulnerabilities.

TECHNICAL DETAILS:

Hewlett Packard Enterprise (HPE) has issued an urgent security update for its Insight Remote Support service, addressing multiple critical vulnerabilities. These flaws, which include XML External Entity (XXE) Injection, Java Deserialization, and Directory Traversal, could potentially allow attackers to access sensitive data, execute arbitrary code, or fully compromise vulnerable systems remotely. The most severe of these vulnerabilities, CVE-2024-53676, carries a CVSS score of 9.8, highlighting the critical nature of the flaw.

Vulnerability Details:

- Directory Traversal vulnerability (CVE-2024-53676): This critical vulnerability, with a CVSS score of 9.8, could allow remote attackers to execute code on affected systems.
- XML External Entity Injection (XXE) flaws (CVE-2024-11622, CVE-2024-53673, CVE-2024-53674, CVE-2024-53675): These vulnerabilities could enable attackers to extract confidential data from affected systems.
- Java Deserialization vulnerability (CVE-2024-53673): This flaw could allow unauthenticated attackers to execute arbitrary code on vulnerable systems.

Affected Versions:

- HPE Insight Remote Support - Prior to v7.14.0.629

Fixed Version:

- HPE Insight Remote Support v7.14.0.629 or later

RECOMMENDATIONS:

Update Insight Remote Support to the fixed version 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?docLocale=en_US&docId=hpesbgn04731en_us