An Lárionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre

NCSC #2412020143

NCSC Advisory

Critical vulnerabilities Hewlett Packard Enterprise (HPE) HPE Insight Remote Support (CVSSv3: 9.8)

2nd, December 2024

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use **TLP:CLEAR** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

Description

Vendor: Hewlett Packard Enterprise (HPE)

Product: HPE Insight Remote Support

CVE ID	CVSS3.0 Score[1]	Published Date
CVE-2024-11622	7.3	2024-11-26
CVE-2024-53673	8.1	2024-11-26
CVE-2024-53674	7.3	2024-11-26
CVE-2024-53675	7.3	2024-11-26
CVE-2024-53676	9.8	2024-11-27

Products affected

Product	Version
HPE Insight Remote Support	Prior to v7.14.0.629

Impact

Multiple security vulnerabilities have been identified in HPE Insight Remote Support. These vulnerabilities could remotely allow a directory traversal, disclosure of information, or code execution.

Common Weakness Enumeration (CWE)[2]:

CWE	Descritpion	CVE
CWE-91	XML Injection (aka Blind XPath Injection)	CVE-2024-11622, CVE-2024-53674, CVE-2024-53675
CWE-552	Files or Directories Accessible to External Parties	CVE-2024-53676
CWE-502	Deserialization of Untrusted Data	CVE-2024-53673

[1] https://www.first.org/cvss/v3.0/specification-document

[2] https://cwe.mitre.org

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

Recommendations

The NCSC strongly reccommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Hewlett Packard Enterprise.

- https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04731en_us

[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog