An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2501030138

# NCSC Advisory

## Critical Vulnerabilities Exist in Windows Lightweight Directory Access Protocol (LDAP)

(CVSS: 9.8)

**3rd, January 2025**

**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

**Published: 2024-12-10**

**Vendor: Microsoft**

**Product: Multiple versions of Windows 10, Windows 11 and Windows Server**

**CVE ID: CVE-2024-49112**

**CVSS Score[1]: 9.8**

**CVE ID: CVE-2024-49113**

**CVSS Score: 7.5**

# Products affected

Full list of products affected for CVE-2024-49112 here and CVE-2024-49113 here

# Impact

- Windows Lightweight Directory Access Protocol (LDAP) Denial of Service Vulnerability
- Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability

**Common Weakness Enumeration (CWE)[2]:**

- CWE-190: Integer Overflow or Wraparound
- CWE-125: Out-of-bounds Read

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

**Used by Ransomware Operators**: N/A

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

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

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

# Recommendations

The NCSC strongly recommends 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 Microsoft.

- https://nvd.nist.gov/vuln/detail/CVE-2024-49112
- https://www.cve.org/CVERecord?id=CVE-2024-49112
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49112
- https://nvd.nist.gov/vuln/detail/CVE-2024-49113
- https://www.cve.org/CVERecord?id=CVE-2024-49113
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49113
- https://www.safebreach.com/blog/ldapnightmare-safebreach-labs-publishes-first-proof-of-concept-exploit-for-cve-2024-49113/