مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Critical Windows LDAP Vulnerabilities

Tracking #:432316699

Date:03-01-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Microsoft disclosed vulnerabilities affecting Windows Lightweight Directory Access Protocol (LDAP), these vulnerabilities pose significant risks to Active Directory Domain Controllers (DCs) and Windows Servers.

TECHNICAL DETAILS:

Microsoft disclosed two vulnerabilities affecting Windows Lightweight Directory Access Protocol (LDAP) as part of their Patch Tuesday updates. These vulnerabilities, CVE-2024-49112 (Remote Code Execution) and CVE-2024-49113 (Denial of Service), pose significant risks to Active Directory Domain Controllers (DCs) and Windows Servers.

Key points:

- CVE-2024-49112: Remote Code Execution vulnerability with a CVSS score of 9.8
- CVE-2024-49113: Denial of Service vulnerability with a CVSS score of 7.5
- Both vulnerabilities affect unpatched Windows Servers, including Domain Controllers
- SafeBreach Labs has developed a proof-of-concept exploit for CVE-2024-49113
- Successful exploitation can lead to server crashes or potential remote code execution

Vulnerability Overview:

- CVE-2024-49112 and CVE-2024-49113 affect the Windows LDAP implementation. The vulnerabilities allow unauthenticated attackers to potentially execute arbitrary code or cause denial of service on affected systems
- Attack Vector: SafeBreach Labs' proof-of-concept for CVE-2024-49113 demonstrates the following attack flow
  - Attacker sends a DCE/RPC request to the victim server
  - Victim is triggered to send a DNS SRV query
  - Attacker's DNS server responds with a hostname and LDAP port
  - Victim sends a broadcast NBNS request to resolve the attacker's hostname
  - Attacker sends an NBNS response with its IP address
  - Victim becomes an LDAP client and sends a CLDAP request to the attacker's machine
  - Attacker sends a malicious CLDAP referral response, causing LSASS to crash and forcing a server reboot

RECOMMENDATIONS:

- Apply Microsoft's December 2024 security updates immediately to all Windows Servers and Domain Controllers
- Monitor for unusual activity involving DNS SRV queries, CLDAP referral responses, and DsrGetDcNameEx2 calls
- Use proof-of-concept tool to assess the systems' vulnerability and Enhance monitoring of Domain Controllers for suspicious activities
- Enhance monitoring of Domain Controllers for suspicious activities and Regularly backup Domain Controllers and test recovery procedures

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://www.safebreach.com/blog/ldapnightmare-safebreach-labs-publishes-first-proof-of-concept-exploit-for-cve-2024-49113/