BLACKSWAN CYBERSECURITY

THREAT ADVISORY

December 18, 2024

Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability (CVE-2024-49112)

SUMMARY

Critical RCE vulnerability affecting the Windows LDAP Client with a CVSS score of 9.8. This vulnerability could allow an unprivileged attacker to run arbitrary code on an Internet-exposed Active Directory Server by sending a specialized set of LDAP calls to the server.

Microsoft recommends that all Active Directory servers be configured to not accept Remote Procedure Calls (RPCs) from untrusted networks in addition to patching this vulnerability.

CVE-2024-49112 - Security Update Guide - Microsoft - Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability

MITIGATION

What actions do customers need to perform to be protected against this vulnerability?

- This vulnerability affects both LDAP clients and servers running an affected version of Windows listed in the Security Updates table. Customers must apply the latest security update for their Windows version to be protected against this vulnerability.

Is there any action a customer can take if they are unable to apply the update?

- Ensure that domain controllers are configured either to not access the internet or to not allow inbound RPC from untrusted networks. While either mitigation will protect your system from this vulnerability, applying both configurations provides an effective defense-in-depth against this vulnerability.

RPC and LDAP are published externally through SSL. What does this mitigation mean in the context of external network connectivity?

- Applying the mitigations will decrease the risk of an attacker successfully convincing or tricking a victim into connecting to a malicious server. If a connection is made, the attacker could send malicious requests to the target over SSL.

How could an attacker exploit this vulnerability?

- A remote unauthenticated attacker who successfully exploited this vulnerability would gain the ability to execute arbitrary code within the context of the LDAP service. However successful exploitation is dependent upon what component is targeted:
    - In the context of **exploiting a domain controller for an LDAP server**, to be successful an attacker must send specially crafted RPC calls to the target to trigger a lookup of the attacker's domain to be performed to be successful.
    - In the context of **exploiting an LDAP client application**, to be successful an attacker must convince or trick the victim into performing a domain controller lookup for the attacker's domain or into connecting to a malicious LDAP server. However, unauthenticated RPC calls would not succeed.

Could an attacker leverage inbound RPC tunnels connected to Windows 11 to successfully exploit this vulnerability?

- Yes, an attacker could use an RPC connection to a domain controller to trigger domain controller lookup operations against the attacker's domain.

REFERENCES

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49112
- https://www.cve.org/CVERecord?id=CVE-2024-49112