THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE

ThreatCure

Cyber Threat Advisory

Windows LDAP RCE

CVE-2024-49112

Description

Windows LDAP RCE

CATEGORY

Vulnerability

SEVERITY

High

Platforms

Window Server, Domain Controller

IMPACT

- Domain Compromise.
- Service Disruption.
- Data Breach Risk.
- Increased Ransomware Threat.
- Regulatory Compliance Issues

A high-severity vulnerability in Windows Lightweight Directory Access Protocol (LDAP), identified as CVE-2024-49112, has been flagged with a CVSS score of 9.8, highlighting its critical threat to enterprise environments. This issue, which affects Windows servers, including Domain Controllers (DCs), was disclosed in Microsoft's December 2024 Patch Tuesday updates. The vulnerability, stemming from an integer overflow in LDAP-related code, allows unauthenticated attackers to crash unpatched servers or execute arbitrary commands through crafted RPC requests. Since Domain Controllers are vital for managing authentication and user privileges in networks, this flaw poses significant security risks.

Microsoft has released patches to resolve the issue, addressing the integer overflow vulnerability. Organizations are advised to deploy the patch without delay, monitor network traffic for potential exploitation attempts, and test their systems. Taking immediate action is essential to prevent potential domain compromises and ransomware attacks.

Mitigation

- Install Microsoft's December 2024 patch without delay. **Reference:** https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49112
- Keep an eye on network activity for unusual DNS SRV queries, CLDAP referral responses, and DsrGetDcNameEx2 calls until the update is fully applied.

ThreatCure

Cyber Threat Advisory

Secure your byte world

Windows LDAP RCE

CVE-2024-49112