Your IT Company

ÍNDICE

Objetivo

Este documento foi desenvolvido e fundamentado nas documentações oficiais do NIST (National Institute Of Standards and Technology), MITRE e CVE.org, que são mundialmente conhecidas na área de cibersegurança como modelos de padronização das melhores práticas de segurança, pesquisa de metodologias de ataques, defesa cibernética e catalogação de novas vulnerabilidades em sistemas operacionais e aplicações.

Análise de Vulnerabilidades: CVE-2024-49112 e CVE-2024-49113 no LDAP

Em dezembro de 2024, o pesquisador de segurança Yuki Chen identificou duas vulnerabilidades críticas no Windows Lightweight Directory Access Protocol (LDAP), que afetaram uma série de versões do Windows. As falhas são CVE-2024-49112, uma vulnerabilidade de execução remota de código (RCE) com uma pontuação CVSS de 9.8, e CVE-2024-49113, uma falha de negação de serviço (DoS) com uma pontuação CVSS de 7.5.

Neste post, vamos explicar essas falhas em detalhes, como os atacantes podem explorá-las e quais são as recomendações de mitigação para garantir que sua infraestrutura esteja protegida.

CVE-2024-49112: Execução Remota de Código (RCE) no LDAP

CVE:CVE-2024-49112

Pontuação CVSS: 9.8 (Crítica)

O Que é a Vulnerabilidade CVE-2024-49112?

A vulnerabilidade CVE-2024-49112 é uma falha no Windows Lightweight Directory Access Protocol (LDAP) que permite a execução remota de código (RCE) através de chamadas de Remote Procedure Call (RPC) malformadas. Isso significa que um atacante remoto e não autenticado pode executar código arbitrário no contexto do serviço LDAP afetado, comprometendo potencialmente todo o sistema.

Como Funciona a Exploração?

A exploração da CVE-2024-49112 depende do componente que o atacante está tentando comprometer.

- No caso de um controlador de domínio LDAP: O atacante deve enviar RPCs malformadas para o servidor LDAP, induzindo-o a realizar uma consulta de domínio para o domínio do atacante. Isso explora a forma como o servidor processa as consultas e, caso bem-sucedido, o atacante pode executar código remoto no servidor.
- No caso de uma aplicação cliente LDAP: O atacante precisa induzir a vítima a realizar uma consulta para o domínio do atacante, o que pode ocorrer se a vítima se conectar a um servidor LDAP malicioso. Vale notar que RPCs não autenticadas não teriam sucesso, ou seja, o atacante precisa de uma maneira de enganar a vítima a se conectar ao servidor LDAP comprometido.

Impacto da Vulnerabilidade:

Se explorada com sucesso, esta falha permite que um atacante tenha controle total sobre o servidor afetado, o que pode levar à execução de comandos arbitrários, comprometendo dados e permitindo a escalada de privilégios. Esta falha é especialmente crítica em controladores de domínio LDAP, que podem ser o coração da infraestrutura de TI de uma organização.

CVE-2024-49113: Negação de Serviço (DoS) no LDAP

CVE: CVE-2024-49113

Pontuação CVSS: 7.5 (Alta)

O Que é a Vulnerabilidade CVE-2024-49113?

A CVE-2024-49113 é uma vulnerabilidade no LDAP que leva a uma negação de serviço (DoS). Ao ser explorada, a falha pode forçar o servidor LDAP a travar, reiniciando automaticamente quando uma resposta maliciosa CLDAP (Connectionless Lightweight Directory Access Protocol) é recebida.

Como Funciona a Exploração?

A vulnerabilidade é chamada LDAPNightmare e pode ser explorada com um PoC (proof-of-concept) já publicado por SafeBreach Labs.

- Fluxo do Ataque: O atacante envia uma requisição DCE/RPC (Distributed Computing Environment/Remote Procedure Call) para o servidor LDAP. Quando o servidor tenta processar a resposta CLDAP malformada, ele faz com que o Local Security Authority Subsystem Service (LSASS) falhe e o servidor se reinicie.
- Requisitos para Exploração: O único pré-requisito para que a falha ocorra é que o servidor DNS do controlador de domínio da vítima tenha conectividade com a Internet. Isso significa que servidores vulneráveis em redes mal protegidas são especialmente suscetíveis ao ataque.

Impacto da Vulnerabilidade

Quando explorada, a CVE-2024-49113 pode causar uma perda de disponibilidade significativa, já que o servidor LDAP será forçado a reiniciar constantemente. Em um ambiente de produção, isso pode resultar em interrupções prolongadas de serviços essenciais, afetando a infraestrutura de rede e comprometendo a operação normal da organização.

Além disso, a CVE-2024-49113 pode ser usada em conjunto com a CVE-2024-49112, como observado por SafeBreach Labs, para converter o ataque de DoS em uma exploração RCE, onde o atacante não só causa uma falha de serviço, mas também ganha controle remoto sobre o servidor afetado.

Quais Versões do Windows São Afetadas?

Ambas as vulnerabilidades afetam várias versões do Windows, incluindo Windows Server e estações de trabalho Windows. Para obter informações detalhadas sobre as versões afetadas, consulte as páginas do Microsoft Security Response Center (MSRC), que fornecem uma lista completa das versões vulneráveis e as atualizações necessárias.

Como Proteger sua Infraestrutura?

Para mitigar as vulnerabilidades CVE-2024-49112 e CVE-2024-49113, as organizações devem adotar as seguintes práticas:

1. Aplicar Atualizações de Segurança

A Microsoft lançou patches para corrigir as falhas de execução remota de código (RCE) e negação de serviço (DoS) associadas a essas vulnerabilidades. A aplicação desses patches é a mitigação mais eficaz para proteger sua infraestrutura contra exploração.

- CVE-2024-49112 (RCE) e CVE-2024-49113 (DoS) podem comprometer servidores LDAP, sendo crucial que os servidores vulneráveis recebam a atualização o quanto antes.
- SafeBreach Labs confirmou que o patch disponível previne a exploração eficazmente. No entanto, como a aplicação de patches em Controladores de Domínio (DC) e Servidores Windows pode afetar ambientes críticos, é essencial adotar uma abordagem cuidadosa, validando a atualização em ambientes de teste antes de implementá-la em produção.

2. Monitoramento de Atividade Suspeita

Até que os patches sejam aplicados em toda a infraestrutura, é importante monitorar a rede e os sistemas para detectar tentativas de exploração. Algumas atividades a serem observadas incluem:

- Respostas CLDAP suspeitas: Fique atento a pacotes CLDAP malformados com valores específicos usados para explorar a falha CVE-2024-49113.
- Chamadas DsrGetDcNameEx2 suspeitas: Essas chamadas RPC são indicativas de tentativas de exploração de CVE-2024-49112.
- Consultas DNS SRV suspeitas: Monitore consultas DNS para detectar sinais de ataque em andamento.

Esses comportamentos podem ser indicativos de tentativas de exploração e devem ser tratados como prioridade, com bloqueio e investigação imediatos.

Esta publicação tem como objetivo orientar a equipe interna e os nossos clientes sobre ameaças emergentes no ambiente cibernético, possibilitando assim ações proativas de prevenção para tornar a infraestrutura de nossas empresas cada vez mais segura.

Produzido por: Harley José Maria Araújo - Consultor de Resposta à Incidentes Pleno