Executive Summary

1 active priority campaign is currently targeting Windows environments running Active Directory Domain Services. A proof-of-concept (PoC) exploit has been publicly released for **CVE-2025-21293**, a **critical privilege escalation vulnerability** patched by Microsoft in January 2025.

Active Threat Campaigns

Campaign	Type	Targets	Key Technique	Priority Action
CVE-2025-21293 AD Privilege Escalation (PRIORITY.25.001)	Privilege Escalation	Organizations running Active Directory Domain Services – all regions	Abuses "Network Configuration Operators" group to register malicious DLLs executed at SYSTEM level via perfmon/WMI	Apply January 2025 Microsoft Patch Tuesday updates immediately

Top 2 Actions This Week

1. Patch All Domain Controllers: Customers immediately apply the January 2025 Microsoft Patch Tuesday update to any on-premises Domain Controllers. This patch removes the "Network Configuration Operators" group's ability to create subkeys under critical registry keys, closing the privilege escalation path.

2. Monitor for Malicious DLL Activity: Watch for unauthorized DLL registration events, especially those triggered by or associated with the "Network Configuration Operators" group. Monitor native Windows tools such as perfmon and WMI for unusual execution behavior that may indicate exploitation.

CVE-2025-21293 – Active Directory Domain Services Elevation of Privilege

This vulnerability stems from a combination of weaknesses in Windows Performance Counters and the built-in "Network Configuration Operators" security group — a lesser-known AD group that is often overlooked in security reviews. An attacker with access to this group can register malicious DLLs. When queried by native Windows tools like Performance Monitor (perfmon) or WMI, those DLLs execute with SYSTEM-level privileges, giving an attacker full control of the affected host.

The vulnerability was discovered in September 2024 and patched in January 2025. With a working PoC now publicly available, the risk of active exploitation is significantly elevated. Microsoft's fix modifies the permissions of the "Network Configuration Operators" group, revoking its ability to create subkeys under sensitive registry locations**.**

Threat Metrics

Activity Trends

- Elevated risk due to public PoC release
- Privilege escalation techniques targeting AD environments
- "Network Configuration Operators" group abuse — likely under monitored in most environments

Indicators of Compromise:

- Unauthorized DLL files registered in Windows Performance Counter paths
- Unexpected SYSTEM-level process execution via perfmon.exe or WMI
- Unusual activity from accounts in the "Network Configuration Operators" group

- **Resources:**
  Microsoft January 2025 Patch Tuesday Advisory
  MITRE ATT&CK: T1543 (Create or Modify System Process), T1574 (Hijack Execution Flow: DLL)