Domain Admin Risk from Windows Kerberos Zero-Day Resolved

TL;DR

Microsoft's fixes a publicly disclosed Windows Kerberos zero-day (CVE-2025-53779, CVSS 7.2) that could allow an authenticated attacker to gain domain admin privileges.

Technical details have been public since May, so exploitation risk is high. Patch immediately.

Overview

This week, Microsoft issued security updates for 107 vulnerabilities across Windows and related products, including a publicly disclosed zero-day flaw in Windows Kerberos (CVE-2025-53779). While Microsoft also addressed multiple high-severity issues, including thirteen critical vulnerabilities, the Kerberos flaw demands immediate attention due to the potential for domain-wide compromise.

Zero-Day – CVE-2025-53779 (CVSS 7.2)

- CVE-2025-53779 is a Windows Kerberos elevation of privilege vulnerability that can allow an authenticated attacker to escalate privileges to a domain administrator over the network. The flaw stems from a relative path traversal issue within Windows Kerberos, requiring the attacker to have elevated access to specific dMSA attributes (msds-groupMSAMembership and msds-ManagedAccountPrecededByLink). Once exploited, this access could give an attacker control over targeted systems across the domain.

- This vulnerability was discovered by Yuval Gordon of Akamai and published in May 2025. Because it was disclosed without a patch prior to today's release, threat actors could already have the technical details needed for exploitation.

Other Vulnerabilities Patched

In addition to CVE-2025-53779, Microsoft resolved dozens of other security issues this month, including remote code execution vulnerabilities in Microsoft Office, DirectX Graphics Kernel, and Windows GDI+, as well as multiple elevation of privilege, information disclosure, spoofing, and denial-of-service flaws.

Aspire Protects

- **Patch** - Apply the updates as soon as possible for CVE-2025-53779.
- Audit accounts with elevated dMSA attribute permissions to limit abuse.
- Monitor for anomalous Kerberos activity, including unexpected privilege escalations or changes to service account.
- Apply additional August patches for other Microsoft products to reduce attack surface.

TTPs to Watch

Privilege Escalation

- Exploitation for Privilege Escalation [T1068] – The attacker may exploit the Kerberos path traversal flaw to elevate privileges to domain administrator.

Credential Access

- Kerberos Ticket Granting Ticket (TGT) Manipulation [T1558.003] – The attacker may modify or forge Kerberos tickets to maintain access after gaining elevated privileges.

Lateral Movement

- SMB/Windows Admin Shares [T1021.002] – The attacker may use elevated rights to move across systems via SMB or Windows administrative shares.

Persistence

- Valid Accounts: Domain Accounts [T1078.002] – The attacker may create or alter domain accounts to maintain persistent access.

IoCs

There are no known IoCs associated with the above vulnerability at this time. Aspire is actively monitoring and will notify customers if any IoCs are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

The Windows Kerberos zero-day patched this month threatens any organization using Active Directory for authentication.

- Education
- Energy & Utilities
- Financial Services
- Healthcare
- Legal & Professional Services
- Manufacturing
- Public Sector
- Retail

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

CVE-2025-53779 - Security Update Guide - Microsoft - Windows Kerberos Elevation of Privilege Vulnerability

BadSuccessor: Abusing dMSA to Escalate Privileges in Active Directory