High-Severity Privilege Escalation in Hybrid Exchange Environments

TL;DR

A new vulnerability (CVE-2025-53786) affects hybrid Exchange Server environments and could let attackers escalate privileges in Microsoft 365 without raising alerts.

If your organization uses Exchange hybrid configurations, patch your on-prem servers and configure the dedicated hybrid app immediately to avoid potential cloud-to-ground domain compromise.

Overview

Microsoft and CISA have issued warnings about a high-severity vulnerability affecting Exchange hybrid deployments. The flaw does not have a CVSS score yet and is tracked as CVE-2025-53786.

CVE-2025-53786 impacts Exchange Server 2016, 2019, and Subscription Edition. If attackers gain admin access to an on-prem Exchange server, they can exploit the shared service principal used in hybrid setups. This allows them to impersonate trusted services in Microsoft 365 without triggering cloud-based audit logs.

Affected Products

- Microsoft Exchange Server 2016 (CU23 + earlier)
- Microsoft Exchange Server 2019 (CU14, CU15 + earlier)
- Microsoft Exchange Server Subscription Edition (prior to April 2025 Hotfix)

This vulnerability can lead to privilege escalation in Exchange Online, bypassing detection mechanisms like Microsoft Purview and standard M365 logging. While no active exploitation has been observed, Microsoft has labeled the vulnerability as “Exploitation More Likely.”

In hybrid Exchange configurations, both the on-prem Exchange Server and Microsoft 365 use a shared service principal to maintain calendar lookups, MailTips, and profile photo sharing. If this shared identity isn’t replaced with Microsoft’s new dedicated hybrid app, attackers can abuse it to forge access tokens and escalate privileges in Exchange Online.

Because Exchange Online trusts calls made from the on-prem server, malicious activity originating on-prem may go undetected in cloud audit logs. Aspire recommends installing Microsoft’s hotfix as soon as possible.

Aspire Protects

- **Patch** - Install Microsoft's April 2025 Exchange Server Hotfix on all affected on-prem Exchange servers.
- Deploy the dedicated Exchange Hybrid App using Microsoft's updated Hybrid Configuration Wizard (HCW).
- Run the Microsoft Exchange Health Checker to ensure patching and configuration are complete.
- Use Microsoft's Service Principal Clean-Up Mode script to remove legacy or unused certificates tied to the shared service principal, even if you're no longer using hybrid coexistence features.
- Disconnect public-facing, unsupported Exchange and SharePoint servers from the internet, especially those that are end-of-life or out-of-support.

TTPs to Watch

Initial Access

- Valid Accounts [T1078] – Attacker may gain control of on-prem Exchange admin accounts.

Privilege Escalation

- Abuse Elevation Control Mechanism [T1548.002] – Forged tokens could elevate attacker rights in Microsoft 365 via the hybrid trust relationship.

Defense Evasion

- Impair Defenses: Disable or Modify Tools [T1562.001] – Malicious activity may not be logged due to cloud's trust in on-prem.

Persistence

- Account Manipulation: Additional Cloud Roles [T1098.003] – Access to Exchange Online can be maintained through abused roles or app registrations.

IoCs

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

Targeted Industries

While no confirmed exploitation of CVE-2025-53786 has been reported, threat actors have historically targeted hybrid Exchange environments in sectors such as:

- Government
- Healthcare
- Education
- Finance
- Energy
- Legal

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

Dedicated Hybrid App: temporary enforcements, new HCW and possible hybrid functionality disruptions | Microsoft Community Hub

Microsoft Releases Guidance on High-Severity Vulnerability (CVE-2025-53786) in Hybrid Exchange Deployments | CISA