مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerability in Exchange Hybrid Deployments

Tracking #:432317575

Date:07-08-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical privilege escalation vulnerability affecting Exchange Server hybrid deployments. This vulnerability could allow attackers with administrative access to an on-premises Exchange Server to escalate their privileges within the connected Exchange Online environment, potentially resulting in a complete domain compromise.

TECHNICAL DETAILS:

A newly disclosed, high-severity vulnerability (CVE-2025-53786) affects Microsoft Exchange Server 2016, 2019, and Subscription Edition deployed in hybrid mode with Exchange Online. Successful exploitation can allow attackers with administrative access to an on-premises Exchange server to escalate privileges and compromise identity integrity in Exchange Online—all without leaving clear audit trails.

Immediate mitigation is required to prevent a potential total domain compromise spanning both on-premises and cloud environments.

Vulnerability Details:

- **CVE:** CVE-2025-53786
- **CVSS Score:** 8.0 High
- The vulnerability stems from the shared service principal identity used for authentication between on-premises Exchange and Exchange Online. If compromised, this trust relationship can be abused to forge tokens or API calls that the cloud environment accepts as legitimate
- **Potential Impact:**
  - Cloud privilege escalation
  - Unauthorized access to Exchange Online
  - Total domain compromise, including hybrid and cloud infrastructure
  - Bypassed auditing/logging mechanisms

Affected Systems:

- Microsoft Exchange Server 2016 (Hybrid Configuration)
- Microsoft Exchange Server 2019 (Hybrid Configuration)
- Microsoft Exchange Server Subscription Edition (SE) (Hybrid Configuration)

RECOMMENDATIONS:

- **Install April 2025 Exchange Server Security Updates**
  - Apply the **Hotfix Updates** released by Microsoft to all affected **on-prem Exchange servers**.
- **Deploy Dedicated Hybrid Application**
  - Follow Microsoft’s guidance to move hybrid authentication to a **dedicated application identity**, reducing exposure of the shared service principal.
- **Reset Shared Service Principal Credentials**
  - Use Microsoft's **Service Principal Clean-Up Mode** to rotate/reset **keyCredentials** for existing hybrid service principals.
- **Run Microsoft Exchange Health Checker**
  - After applying fixes and configuration changes, run the **Health Checker** tool to

ensure all mitigation steps have been correctly implemented.

- **Disconnect Unsupported or EOL Servers**
  - Isolate or decommission any **end-of-life (EOL)** Exchange or SharePoint servers that are publicly accessible.
- **Harden On-Prem Environments**
  - Apply best practices for Exchange security, including restricting administrative access, hardening PowerShell, and monitoring unusual traffic between on-prem and cloud.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.cisa.gov/news-events/alerts/2025/08/06/microsoft-releases-guidance-high-severity-vulnerability-cve-2025-53786-hybrid-exchange-deployments
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53786