Security Advisory 2025-030

High Severity Vulnerability in Microsoft Exchange

2025-08-08 — v1.1

TLP:CLEAR

History:

- *08/08/2025 — v1.0 – Initial publication*
- *08/08/2025 — v1.1 – Updated information*

Summary

On August 6, 2025, Microsoft issued an advisory for a high-severity vulnerability affecting Microsoft Exchange hybrid environments [1]. The vulnerability tracked as **CVE-2025-53786** allows an attacker with administrative access to an on-premises Exchange Server to escalate privileges into the connected Exchange Online environment. The vulnerability can impact the confidentiality, integrity, and availability of affected systems.

Technical Details

An attacker with admin privileges on an on-premise Exchange server can potentially forge or manipulate trusted tokens or API calls that the cloud side will accept as legitimate. This technique allows the attackers to spread laterally from the local network into the organisation's cloud environment, potentially compromising the organisation's entire active directory and infrastructure [6].

Products Affected

The vulnerability affects the following Microsoft Exchange Servers in Hybrid Exchange Deployments:

- Microsoft Exchange Server 2016 Cumulative Update 23 versions earlier than 15.01.2507.055
- Microsoft Exchange Server 2019 Cumulative Update 14 versions earlier than 15.02.1544.025
- Microsoft Exchange Server 2019 Cumulative Update 15 versions earlier than 15.02.1748.024
- Microsoft Exchange Server Subscription Edition RTM versions earlier than 15.02.2562.017

Recommendations

It is strongly recommended to apply the follow the vendor guidance [1]:

- If using Exchange hybrid, review Microsoft's guidance to determine if your Microsoft hybrid deployments are potentially affected and available for a Cumulative Update (CU) [2].
- Install Microsoft's April 2025 Exchange Server Hotfix Updates [3] on the on-premise Exchange server and follow Microsoft's configuration instructions to deploy the dedicated Exchange hybrid app [4].
- For organisations using Exchange hybrid (or have previously configured Exchange hybrid but no longer use it), review Microsoft's Service Principal Clean-Up Mode [4] for guidance on resetting the service principal's `keyCredentials` .
- Upon completion, run the Microsoft Exchange Health Checker [5] to determine if further steps are required.

Threat Hunting

The KQL query below detects potential abuse of the `graph.windows.net` API through impersonation — later fixed by Microsoft [7].

```
AuditLogs
| where not(OperationName has "group")
| where not(OperationName == "Set directory feature on tenant")
| where InitiatedBy has_all ( "Office 365 Exchange Online","user")
| where InitiatedBy.user.displayName == "Office 365 Exchange Online"
```

References

[1] https://msrc.microsoft.com/update-guide/advisory/CVE-2025-53786

[2] https://techcommunity.microsoft.com/blog/exchange/exchange-server-security-changes-for-hybrid-deployments/4396833

[3] https://techcommunity.microsoft.com/blog/exchange/released-april-2025-exchange-server-hotfix-updates/4402471

[4] https://learn.microsoft.com/en-us/Exchange/hybrid-deployment/deploy-dedicated-hybrid-app

[5] https://microsoft.github.io/CSS-Exchange/Diagnostics/HealthChecker/

[6] https://www.bleepingcomputer.com/news/security/cisa-orders-fed-agencies-to-patch-new-cve-2025-53786-exchange-flaw/

[7] https://i.blackhat.com/BH-USA-25/Presentations/US-25-Mollema-Advanced-AD-to-Entra-ID-lateral-movement-techniques-Wednesday.pdf