關於 2021.03 的 Exchange Server 零時差漏洞攻擊

Q:哪些版本的 Exchange 伺服器會受到影響？

A: Microsoft 發佈的安全性更新可以解決報告中的安全性漏洞，這些漏洞會影響包含: Exchange Server 2013、Exchange Server 2016 和 Exchange Server 2019。為了深度防禦，我們也發佈了 Exchange Server 2010 的更新。

Q:這些漏洞會影響 Exchange Online 嗎？

A:不會。使用 Exchange Online 的客戶不會受到這些漏洞的影響，也不需要進行額外的動作。

Q:在本次提供的 Exchange 安全性更新中，將解決多少安全性漏洞？

A:本次的安全性更新版本針對影響 Exchange Server 的七個安全性漏洞進行修復。其中，已知有四種對本機 Exchange 伺服器的攻擊有限且有針對性。

Q:這些漏洞的嚴重性、影響和 Base CVSS 分數是什麼？

A:本次漏洞包含嚴重等級被評為「critical」的 Remote Code Execution， 最高的 Base CVSS 分數是 9.1。

Q:是否可以確認 Exchange Server 漏洞已經的有在網路上有被利用呢？

A:是的。Microsoft 注意到此次為國家級惡意攻擊，主要針對本機 Exchange 伺服器進行目標式攻擊。

Q:我需要準備什麼，讓 Exchange Server 準備好於三月份更新嗎？

A: Microsoft 為 Exchange Server 2016 和 Exchange Server 2019 提供了兩個最新的 Cumulative Updates (CUs)支援，以及為 Exchange Server 2010 和 Exchange Server 2013 提供了最新的 Update Rollup (UR)的支援。Exchange 伺服器若採用受支援的 UR 或 CU，即為最新版本。在安裝任何安全性更新之前，非最新版本的 Exchange 伺服器需要安裝受支援的 UR 或 CU。 Exchange 管理員應考慮到，若要更新過時的 Exchange 伺服器需要額外時間。下方的 Exchange Team 部落格文章將提供更多詳細資訊。

Q:我有什麼方式可以判斷哪個 Exchange 伺服器可以直接安裝安全性更新，那些則需要先安裝受支援的 UR 或 CU？

A: 是的。您可以使用 Exchange Server Health Checker 的程式碼（可以在 GitHub 中下載的最新版本）。這些程式碼將告訴您，您的本機 Exchange Server 是否為過時的。

Q: 那些 Exchange 伺服器需要優先處理更新動作？

A: 是的。暴露在網路上的 Exchange 伺服器將是高風險伺服器，所以因此應優先處理。下方的 Exchange Team 部落格文章將提供您更多資訊。

Q:這些漏洞是否有 workaround 解決方法？

A: 若您延後安裝安全性更新，唯一的解決方式就是將 Exchange Servers 從對外網路中移除，直到能夠安裝三月的安全性更新為止。

Q:我要如何辨識我的 Exchange 伺服器是否有因為這些漏洞遭受入侵？

A: 下方的 **Microsoft Threat Intelligence Center (MSTIC)**部落格文章中，提供安全專家技術指南，以便獵捕任何涉及這些漏洞的入侵。

Q:在安裝安全性更新後，是否需要重新啟動 Exchange 伺服器？

A: 是的。當完成安裝安全性更新後，需要重新啟動 Exchange 伺服器，才能啟用安全性更新。

Q:影響 Exchange 伺服器的漏洞是否和近期影響 SolarWinds 的攻擊有關？

A: 不是。我們沒有注意到影響 Exchange Server 的漏洞和近期 SolarWinds 攻擊的關聯性。

Q: 您是否可以告訴我關於這個受到國家級惡意行為者利用此次事件的資訊？

A: 我們在部落格文章中提供目前可以分享的更多資訊。請參考：

MSTIC blog: https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/ 和
On the Issues (MOTI) blog: https://blogs.microsoft.com/on-the-issues/?p=64505.

Q:我可以在哪裡找到關於這些 Exchange Server 漏洞的可信資訊？

A: 關於漏洞細節的最佳資源都在 CVE 的頁面，以及底下 MSTIC 的部落格文章中。

Related Resources

- **Exchange Team Blog**: https://techcommunity.microsoft.com/t5/exchange-team-blog/released-march-2021-exchange-server-security-updates/ba-p/2175901
- **MSRC blog**: https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server
- **MSTIC blog:** https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
- **On the Issues (MOTI) blog**: https://blogs.microsoft.com/on-the-issues/?p=64505
- **CVE-2021-26855 | Microsoft Exchange Server Remote Code Execution Vulnerability**: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855
- **CVE-2021-26857 | Microsoft Exchange Server Remote Code Execution Vulnerability**: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26857
- **CVE-2021-26858 | Microsoft Exchange Server Remote Code Execution Vulnerability**: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26858
- **CVE-2021-27065 | Microsoft Exchange Server Remote Code Execution Vulnerability**: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-27065
- **The Security Update Guide**: http://aka.ms/securityupdateguide