

狀態:	New-新增	開始日期:	2025-08-01
優先權:	High	完成日期:	2025-12-31
被分派者:		完成百分比:	89%
分類:	執行階段	預估工時:	0:00 小時
版本:		耗用工時:	0:00 小時
概述 ADPT_TAHO_Remediation Tracker Severity Ref. Weakness NNN bookmark20250526222819601367469548 "Cleartext Passwords Stored in Domain Attributes Several users, including domain admins, store their passwords in cleartext in domain attributes. " NN "4.3.2 MITRE-T1558 " "Domain Admin Vulnerable to Kerberoasting Attack It is possible to obtain the encrypted Kerberos service ticket of a domain admin for offline password cracking. " NN bookmark20250528021100422251172311 "Dangerous Permission over Accounts with Replication Rights All domain users have ForceChangePassword permission against three accounts which have DCSync ability. " NN bookmark20250528105554721728147917 "Dangerous Permisson over GPO that applies to object with high privileges All domain users can modify GPO that will affect an OU containing domain admins." bookmark20250527015003600759977664 "Sensitive Data Stored in Domain Controller ' s Network Shares " N bookmark20230424152553354013409667 "Privileged Accounts with Never Expiring Passwords " "4.7.3 CWE-16 CWE-284 " "SMB NULL Session Authentication allowed on Domain Controllers The SMB service on domain controllers allows users to authenticate using a NULL session, meaning that no user credentials need to be supplied to the server. " N bookmark2025052801463337292181788 "Use of ""Pre-Windows 2000 Compatible Access"" group " N bookmark20250529113929916258883991 "ADCS Web Enrollment Enabled for high-privileged accounts " N "4.7.2 KB2696547 " "SMB version 1 in use on Domain Controller			

"	
N bookmark20250526231504779653815004	"Krbtgt Password Unchanged for over 1 year
"	
N bookmark20250528093106041557187875	"Dangerous Permission over Domain Context Root
"	
N bookmark20250527150517990578686946	"Non-restricted Domain Join with Excessive Machine Account Quota
"	
bookmark20250528012341779511785327	Presence of user principals in Schema Admins group
bookmark20230424152530055619155201	"Privileged account outside from 'Protected Users' group
"	
bookmark2025052818064551592624366	"Overly Permissive Non-Privileged Accounts
"	
bookmark20230424152607541378202907	"Object Owner Anomalies
"	
bookmark20250528113440590525911882	"Dangerous Permission over Privileged Objects Containers
"	
bookmark20250528101140588319445694	"Dangerous Permission over MicrosoftDNS server objects
"	
bookmark20250527172903274457208324	"Dangerous Permission over Domain Controllers Group
"	
bookmark2025052717152717274892035	"Dangerous Permission over adminSDHolder
"	
bookmark20250527164529819756743971	"Dangerous Permission over DNSAdmins Group
"	
子任務:	
專案資訊 # 1065: Cleartext Passwords Stored in Domain Attributes	Resolved-解決
專案資訊 # 1066: Domain Admin Vulnerable to Kerberoasting Attack	Resolved-解決
專案資訊 # 1067: Dangerous Permission over Accounts with Replicati...	New-新增
專案資訊 # 1068: Dangerous Permisson over GPO that applies to obje...	Resolved-解決
專案資訊 # 1069: Dangerous Permisson over GPO that applies to obje...	Resolved-解決
專案資訊 # 1070: Dangerous Permisson over GPO that applies to obje...	Resolved-解決
專案資訊 # 1071: Sensitive Data Stored in Domain Controller ' s Netw...	Resolved-解決
專案資訊 # 1072: Privileged Accounts with Never Expiring Passwords	Resolved-解決
專案資訊 # 1073: SMB NULL Session Authentication allowed on Domain...	Resolved-解決
專案資訊 # 1074: Use of ""Pre-Windows 2000 Compatible Access	Resolved-解決
專案資訊 # 1075: ADCS Web Enrollment Enabled for high-privileged a...	Resolved-解決
專案資訊 # 1076: SMB version 1 in use on Domain Controller	Resolved-解決
專案資訊 # 1077: Krbtgt Password Unchanged for over 1 year	Resolved-解決
專案資訊 # 1078: Dangerous Permission over Domain Context Root	Resolved-解決
專案資訊 # 1079: Non-restricted Domain Join with Excessive Machine...	Resolved-解決
專案資訊 # 1080: Presence of user principals in Schema Admins group	Resolved-解決
專案資訊 # 1081: Privileged account outside from 'Protected Users...	Resolved-解決
專案資訊 # 1082: Privileged account outside from 'Protected Users...	Resolved-解決
專案資訊 # 1083: Overly Permissive Non-Privileged Accounts	Resolved-解決
專案資訊 # 1084: Object Owner Anomalies	In process-進行中
專案資訊 # 1085: Dangerous Permission over Privileged Objects Cont...	In process-進行中
專案資訊 # 1086: Dangerous Permission over MicrosoftDNS server obj...	Resolved-解決
專案資訊 # 1087: Dangerous Permission over Domain Controllers Group	Resolved-解決
專案資訊 # 1088: Dangerous Permission over adminSDHolder	Resolved-解決

歷史

#1 - 2025-11-10 13:27 - Joy Liao

- 子任務 #1065 已新增

#2 - 2025-11-10 13:28 - Joy Liao

- 子任務 #1066 已新增

#3 - 2025-11-10 13:28 - Joy Liao

- 子任務 #1067 已新增

#4 - 2025-11-10 13:28 - Joy Liao

- 子任務 #1068 已新增

#5 - 2025-11-10 13:29 - Joy Liao

- 子任務 #1069 已新增

#6 - 2025-11-10 13:29 - Joy Liao

- 子任務 #1070 已新增

#7 - 2025-11-10 13:29 - Joy Liao

- 子任務 #1071 已新增

#8 - 2025-11-10 13:29 - Joy Liao

- 子任務 #1072 已新增

#9 - 2025-11-10 13:30 - Joy Liao

- 子任務 #1073 已新增

#10 - 2025-11-10 13:30 - Joy Liao

- 子任務 #1074 已新增

#11 - 2025-11-10 13:30 - Joy Liao

- 子任務 #1075 已新增

#12 - 2025-11-10 13:30 - Joy Liao

- 子任務 #1076 已新增

#13 - 2025-11-10 13:31 - Joy Liao

- 子任務 #1077 已新增

#14 - 2025-11-10 13:31 - Joy Liao

- 子任務 #1078 已新增

#15 - 2025-11-10 13:31 - Joy Liao

- 子任務 #1079 已新增

#16 - 2025-11-10 13:31 - Joy Liao

- 子任務 #1080 已新增

#17 - 2025-11-10 13:31 - Joy Liao

- 子任務 #1081 已新增

#18 - 2025-11-10 13:32 - Joy Liao

- 子任務 #1082 已新增

#19 - 2025-11-10 13:32 - Joy Liao
- 子任務 #1083 已新增

#20 - 2025-11-10 13:32 - Joy Liao
- 子任務 #1084 已新增

#21 - 2025-11-10 13:32 - Joy Liao
- 子任務 #1085 已新增

#22 - 2025-11-10 13:32 - Joy Liao
- 子任務 #1086 已新增

#23 - 2025-11-10 13:33 - Joy Liao
- 子任務 #1087 已新增

#24 - 2025-11-10 13:33 - Joy Liao
- 子任務 #1088 已新增

#25 - 2025-11-10 13:33 - Joy Liao
- 子任務 #1089 已新增

檔案

ADPT_TAHO_Remediation Tracker (2).xlsx	397 KB	2025-11-10	Joy Liao
--	--------	------------	----------