User Account Modification, Data Component DC0010

Archived: 2026-04-05 13:44:20 UTC

auditd:SYSCALL usermod, groupmod, passwd auditd:SYSCALL SYSCALL for usermod or /etc/group file modification auditd:SYSCALL usermod, or account rename system calls AWS:CloudTrail UpdateLoginProfile AWS:CloudTrail AttachUserPolicy, CreatePolicyVersion, PutRolePolicy AWS:CloudTrail AttachUserPolicy AWS:CloudTrail CreateAccessKey AWS:CloudTrail role privilege expansion detected azure:audit Operation IN ("Add device", "Add registered users to device", "Add registered owner to device") azure:audit Add member to role azure:audit Rename user azure:audit Add service principal credentials, app password added, app role assignment azure:policy DisableMfaPolicy or change to ConditionalAccess rules azure:signinlogs unusual role assumption or elevation path gcp:audit Admin Activity > Role Change or Sharing Change gcp:audit google.iam.admin.v1.RoleAssignment gcp:audit Set Gmail Delegation gcp:audit iam.serviceAccounts.keys.create, os-login.sshPublicKeys.add gcp:audit API Key Created, OAuth Client Registered kubernetes:audit create or update events for RoleBinding or ClusterRoleBinding objects linux:syslog sudo or su access prior to content change m365:audit Add member to role, Add app role assignment m365:unified Admin Activity > Role Change or Sharing Change m365:unified Set-ADUser OR Set-ADAccountControl m365:unified User excluded from MFA or MFA method registered m365:unified Add member to role, Set-Mailbox m365:unified Set-MailboxAuditBypassAssociation or disabling Advanced Auditing m365:unified New agent registration by non-admin user m365:unified Add-MailboxPermission, UpdateFolderPermissions m365:unified Set-Mailbox, Set-InboxRule, Set-MailboxFolderPermission macos:unifiedlog com.apple.accountsd, com.apple.opendirectoryd macos:unifiedlog Process execution or directory service changes Okta:SystemLog user.account.privilege.grant saas:okta User Attribute Modified / Role Assignment Changed saas:okta user.lifecycle.delete, user.account.lock saas:okta admin role granted outside approved workflows saas:zoom DisableMFA or RegisterNewFactor WinEventLog:Security EventCode=4738, 4728, 4670 WinEventLog:Security EventCode=4723, 4724, 4740 WinEventLog:Security EventCode=4704 WinEventLog:Security EventCode=4728, 4729, 4732, 4733, 4756, 4757

Source: https://attack.mitre.org/datacomponents/DC0010