Abuse Elevation Control Mechanism: Temporary Elevated Cloud Access, Sub-technique T1548.005 - Enterprise

Archived: 2026-04-05 17:22:16 UTC

Adversaries may abuse permission configurations that allow them to gain temporarily elevated access to cloud resources. Many cloud environments allow administrators to grant user or service accounts permission to request just-in-time access to roles, impersonate other accounts, pass roles onto resources and services, or otherwise gain short-term access to a set of privileges that may be distinct from their own.

Just-in-time access is a mechanism for granting additional roles to cloud accounts in a granular, temporary manner. This allows accounts to operate with only the permissions they need on a daily basis, and to request additional permissions as necessary. Sometimes just-in-time access requests are configured to require manual approval, while other times the desired permissions are automatically granted.[1]

Account impersonation allows user or service accounts to temporarily act with the permissions of another account. For example, in GCP users with the `iam.serviceAccountTokenCreator` role can create temporary access tokens or sign arbitrary payloads with the permissions of a service account, while service accounts with domain-wide delegation permission are permitted to impersonate Google Workspace accounts.[2][3][4][5] In Exchange Online, the `ApplicationImpersonation` role allows a service account to use the permissions associated with specified user accounts.[6]

Many cloud environments also include mechanisms for users to pass roles to resources that allow them to perform tasks and authenticate to other services. While the user that creates the resource does not directly assume the role they pass to it, they may still be able to take advantage of the role's access -- for example, by configuring the resource to perform certain actions with the permissions it has been granted. In AWS, users with the `PassRole` permission can allow a service they create to assume a given role, while in GCP, users with the `iam.serviceAccountUser` role can attach a service account to a resource.[7][2]

While users require specific role assignments in order to use any of these features, cloud administrators may misconfigure permissions. This could result in escalation paths that allow adversaries to gain access to resources beyond what was originally intended.[8][9]

Note: this technique is distinct from Additional Cloud Roles, which involves assigning permanent roles to accounts rather than abusing existing permissions structures to gain temporarily elevated access to resources. However, adversaries that compromise a sufficiently privileged account may grant another account they control Additional Cloud Roles that would allow them to also abuse these features. This may also allow for greater stealth than would be had by directly using the highly privileged account, especially when logs do not clarify when role impersonation is taking place.[10]

Source: https://attack.mitre.org/techniques/T1548/005