Sign in

OTRF / **Set-AuditRule** Public

Notifications · Fork 23 · Star 88

Code · Issues 1 · Pull requests · Actions · Projects · Security · Insights

Set-AuditRule / rules / registry / aad_connect_health_service_agent.yml

20 lines (20 loc) · 806 Bytes

Code · Blame · Raw

```yaml
title: Azure AD Connect Health Service Agent
id: b3068822-704a-43a8-8b6f-970148462c8d
status: experimental
description: A threat actor might want to read information about the Azure AD connect health servic
references:
    - https://o365blog.com/post/hybridhealthagent/
    - https://github.com/Gerenios/AADInternals/blob/master/HybridHealthServices_utils.ps1#L457-L461
author: Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research), MSTIC R&D
date: 2020/06/07
rule_category: registry
rule:
    registry_paths:
        - 'HKLM:\SOFTWARE\Microsoft\ADHealthAgent'
    well_known_sid_type: BuiltinAdministratorsSid
    rights:
        - ReadKey
    inheritance_flags: ContainerInherit
    propagation_flags: None
    audit_flags:
        - Success
```