



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\_monitoring\_agent.yml



20 lines (20 loc) · 805 Bytes

Code Blame Raw Copy Download Toggle

```
1 title: Azure AD Connect Health Monitoring Agent
2 id: e6393e38-6c3e-4bce-8696-3d72d37c2ec2
3 status: experimental
4 description: A threat actor might want to read information about the endpoint Microsoft monitoring
5 references:
6   - https://o365blog.com/post/hybridhealthagent/
7   - https://github.com/Gerenios/AADInternals/blob/master/HybridHealthServices_utils.ps1#L457-L461
8 author: Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research), MSTIC R&D
9 date: 2020/08/25
10 rule_category: registry
11 rule:
12   registry_paths:
13     - 'HKLM:\SOFTWARE\Microsoft\Microsoft Online\Reporting\MonitoringAgent'
14   well_known_sid_type: BuiltinAdministratorsSid
15   rights:
16     - ReadKey
17   inheritance_flags: None
18   propagation_flags: None
19   audit_flags:
20     - Success
```

