

apache cloudstack *

Description:

The CloudStack integration API service allows running its unauthenticated API server (usually on port 8096 when configured and enabled via integration.api.port global setting) for internal portal integrations and for testing purposes. By default, the integration API service port is disabled and is considered disabled when integration.api.port is set to 0 or negative. Due to an improper initialisation logic, the integration API service would listen on a random port when its port value is set to 0 (default value). An attacker that can access the CloudStack management network could scan and find the randomised integration API service port and exploit it to perform unauthorised administrative actions and perform remote code execution on CloudStack managed hosts and result in complete compromise of the confidentiality, integrity, and availability of CloudStack managed infrastructure. Users are recommended to restrict the network access on the CloudStack management server hosts to only essential ports. Users are recommended to upgrade to version 4.18.2.1, 4.19.0.2 or later, which addresses this issue.

Main problems:

665 no CWE Description available