NVD DB Update

CVE-2024-38346 - Score: 9.8

Components:

apache cloudstack *

Description:

The CloudStack cluster service runs on unauthenticated port (default 9090) that can be misused to run arbitrary commands on targeted hypervisors and CloudStack management server hosts. Some of these commands were found to have command injection vulnerabilities that can result in arbitrary code execution via agents on the hosts that may run as a privileged user. An attacker that can reach the cluster service on the unauthenticated port (default 9090), can exploit this to 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 to the cluster service port (default 9090) on a CloudStack management server host to only its peer CloudStack management server hosts. Users are recommended to upgrade to version 4.18.2.1, 4.19.0.2 or later, which addresses this issue.

Main problems:

94 "Improper Control of Generation of Code (’Code Injection’)"