Severity

High

Analysis Summary

CVE-2022-22973 CVSS:7.8

VMware Workspace ONE Access and VMware Identity Manager could allow a local authenticated attacker to gain elevated privileges on the system. An attacker could exploit this vulnerability to gain root privileges.

CVE-2022-22972 CVSS:9.8

VMware Workspace ONE Access, VMware Identity Manager, and VMware vRealize Automation could allow a remote attacker to bypass security restrictions. By sending a specially-crafted request, an attacker could exploit this vulnerability to obtain administrative access.

This is a critical vulnerability. Patch Now!

Impact

- Privilege Escalation
- Security Bypass

Indicators Of Compromise

CVE

- CVE-2022-22972
- CVE-2022-22973

Affected Vendors

- VMware

Affected Products

- VMware Identity Manager 3.3.3
- VMware Workspace ONE Access 21.08.0.1
- VMware Workspace ONE Access 21.08.0.0
- VMware Workspace ONE Access 20.10.0.1
- VMware Identity Manager (vIDM)
- VMware vRealize Automation (vRA)
- VMware Cloud Foundation
- vRealize Suite Lifecycle Manager

Remediation

Refer to VMware Security Advisory for patch, upgrade or suggested workaround information.

VMware Security Advisory

Procedure to apply the Workaround:

1. Run View-Active-Admin-users.sql to see all administrators (readonly administrators also included) and run View-Active-Local-users.sql to see all local users who will be disabled. Make sure that View-Active-Admin-users.sql shows at least 1 provisioned (usually from a Directory) administrator
2. Run Disable_All_Local_users.sql to disable all local users and administrators
3. Run View-Active-Admin-users.sql to see which administrators now remain active. Only provisioned (usually Directory users) userType administrators should show here.
4. Login to Workspace ONE Access/VMware Identity Manager appliance using a sshclient as root user. Restart the service using the command “service horizon-workspace restart”. Repeat this process for all appliances in your environment.
5. Until the hotfixes are applied, do not create any new local users.

Procedure to revert the Workaround:

Use these steps only after applying the Hotfixes or if there is a lock out

1. Run Reenable_Disabled_Users.sql to enable the previously disabled users
2. Run View-Active-Admin-users.sql and View-Active-Local-users.sql to confirm that local users and administrators have been re-enabled