KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Critical Auth Bypass bug CVE-2022-31656 affects VMware products

Tracker ID: TN0805 **Date:** 04/August/2022 **Category:** Vulnerability **Industry:** All **Region**: All

Background

VMware has issued an administrator advisory to resolve a critical authentication bypass security vulnerability affecting local domain users in multiple products, which could allow unauthenticated attackers to get administrator privileges. The CVE-2022-31656 flaw vulnerability has been found to affect VMware Workspace ONE Access, Identity Manager, and vRealize Automation. This security vulnerability has been rated critical by VMware, with a CVSSv3 base score of 9.8 out of 10.

The flaw affects local domain users and requires a remote attacker to have network access to a vulnerable user interface. An attacker can use the weakness to circumvent authentication and get administrator access. The identified solution to eliminate the vulnerabilities in your environment is to apply the updates given in VMSA-2022-0021. Publicly accessible solutions do not fix the vulnerabilities and can make patching more difficult.

Other updates were also released for vulnerable systems to address security weaknesses such as privilege escalation to "root" and remote code execution (CVE-2022-31658, CVE-2022-31659, and CVE-2022-31665) (CVE-2022-31660, CVE-2022-31661, and CVE-2022-31664).

Analysis

CVE ID	Severity	CVSS Score
CVE-2022-31656	Critical	9.8

Affected Products and Versions

- VMware Workspace ONE Access (Access)
- VMware Identity Manager (vIDM)
- VMware vRealize Automation (vRA)

Recommendations

- Immediately identify the vulnerable instances and apply the below vendor-provided fixes as soon as possible.
- To remediate CVE-2022-31656, apply the patches shared by VMware.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Critical Auth Bypass bug CVE-2022-31656 affects VMware products

Tracker ID: TN0805 **Date:** 04/August/2022 **Category:** Vulnerability **Industry:** All **Region**: All

References

- Sergiu Gatlan, VMware urges admins to patch critical auth bypass bug immediately, Bleeping Computer, 3rd August 2022, External Link (www.bleepingcomputer.com).
- VMware Inc, Authentication Bypass Vulnerability (CVE-2022-31656), 2nd August 2022, External Link (www.vmware.com).

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176 471 471

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia