



# 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 VMSEA-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](#).

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2022 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.

#KPMGjosh

home.kpmg/in

Follow us on [home.kpmg/in/socialmedia](#)





# 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, 3<sup>rd</sup> August 2022, External Link ([www.bleepingcomputer.com](http://www.bleepingcomputer.com)).
- VMware Inc, Authentication Bypass Vulnerability (CVE-2022-31656), 2<sup>nd</sup> August 2022, External Link ([www.vmware.com](http://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

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2022 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.

#KPMGjosh

home.kpmg/in

Follow us on [home.kpmg/in/socialmedia](http://home.kpmg/in/socialmedia)

