

Overall rating: Medium



This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a vulnerability in VMware Workspace ONE Launch. The vulnerability affects VMware Workspace ONE Launcher 22.x and 23.x.

Technical Details

A privilege escalation vulnerability in VMware Workspace ONE Launch was responsibly reported to VMware. A malicious actor with physical access to Workspace ONE Launcher could utilize the Edge Panel feature to bypass setup to gain access to sensitive information. Updates are available to remediate this vulnerability in affected VMware products.

Exploitability Metrics

Attack Vector: Physical
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **MEDIUM** risk. A software update exists to address this risk.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify [VRM](#) with any questions or concerns you may have.

References

- [CVE-2023-34064](#)
- [VMSA-2023-0027](#)
- [VRM Vulnerability Reports](#)