November 1, 2023

Overall Rating - High

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware VMware has published a security advisory to address vulnerabilities in the following product:

- VMware Workspace ONE UEM 2302 – versions prior to 23.2.0.10
- VMware Workspace ONE UEM 2212 – versions prior to 22.12.0.20
- VMware Workspace ONE UEM 2209 – versions prior to 22.9.0.29
- VMware Workspace ONE UEM 2206 – versions prior to 22.6.0.36
- VMware Workspace ONE UEM 2203 – versions prior to 22.3.0.48
-

Technical Details

VMware Workspace ONE UEM console contains an open redirect vulnerability. VMware has evaluated the severity of this issue to be in the Important severity range with a maximum CVSSv3 base score of 8.8.

Known Attack Vectors
A malicious actor may be able to redirect a victim to an attacker and retrieve their SAML response to login as the victim user.

Resolution
To remediate CVE-2023-20886 apply the patches listed in the 'Fixed Version' column of the 'Response Matrix' below.

Workarounds
None.

These vulnerabilities are rated as an overall **High** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify VRM with any questions or concerns you may have.

References

- CVE-2023-20886
- VMSA-2023-0025
- VMware Security Advisories

Please note that we will be transitioning to a new site on August 31, 2023, where we will post the vulnerability reports.

You will be able to find all the reports that we have published as well as all future reports here: Cybersecurity Alerts