NATIONAL CSIRT-CY

CVE-2025-25231 **15/9/2025**

Secondary Context Path Traversal Vulnerability

Executive Summary

Omnissa Workspace ONE UEM contains a Secondary Context Path Traversal Vulnerability. A malicious actor may be able to gain access to sensitive information by sending crafted GET requests (read-only) to restricted API endpoints.

Analysis

The product uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the product does not properly neutralize special elements within the pathname that can cause the pathname to resolve to a location that is outside of the restricted directory.

Please follow the link below for further information:

https://kb.omnissa.com/s/article/6001021?lang=en_US

Common Weakness Enumeration

https://cwe.mitre.org/data/definitions/22.html

Common Vulnerabilities & Exposures

https://nvd.nist.gov/vuln/detail/CVE-2025-25231

Solutions

Product	Version	CVE Identifier
Workspace ONE UEM console	24.10	CVE-2025-25231
Workspace ONE UEM console	24.06	CVE-2025-25231
Workspace ONE UEM console	24.02	CVE-2025-25231
Workspace ONE UEM console	23.10	CVE-2025-25231

Please distribute this information among your subsidiaries and partners, and also share with us any pertinent information and findings you may have (e.g IOCs, TTPs etc)

The Digital Security Authority extends its appreciation for the continued collaboration.

Disclaimer

Organizations are advised to consult with relevant cybersecurity professionals and follow best practices for their specific environments