April 5, 2024

Overall rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a HPE Unified OSS Console Assurance Monitoring (UOCAM) vulnerability. The vulnerability affects HPE Unified OSS Console (UOC) versions prior to v3.1.4.

Technical Details

Potential security vulnerabilities have been identified in HPE UOCAM. These vulnerabilities could be exploited to allow Remote Authentication Bypass, Remote Denial of Service (DoS), Local Disclosure of Sensitive Information, Local Unauthorized Disclosure of Information, Local Server-Side Request Forgery (SSRF), and Remote Server-Side Request Forgery (SSRF).

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **CRITICAL** 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-2021-44906, CVE-2024-28176, , CVE-2024-28849, , CVE-2023-6378, CVE-2024-22257, CVE-2024-22259
- HPESBGN04629 rev.1 - HPE Unified OSS Console Assurance Monitoring (UOCAM), Multiple Vulnerabilities
- HPE Security Bulletin Library
- VRM Vulnerability Reports