Hive Pro

Threat Level

Amber

THREAT ADVISORY

VULNERABILITY REPORT

Authentication Bypass Vulnerabilities in VMware Workspace ONE Assist

Date of Publication	Admiralty Code	TA Number
November 9, 2022	A1	TA2022249

Summary

First Seen: November 8, 2022
Affected Product: VMware Workspace ONE Assist
Impact: Gain administrative rights without authentication

CVEs

CVE	NAME	PATCH
CVE-2022-31685	Authentication Bypass vulnerability	✓
CVE-2022-31686	Broken Authentication Method vulnerability	✓
CVE-2022-31687	Broken Access Control vulnerability	✓

Vulnerability Details

Several security vulnerabilities exist in VMware's Workspace ONE Assist solution, some of which can be exploited for authentication bypassing to gain admin-level access.

A vulnerability in VMware Workspace ONE Assist, CVE-2022-31685, could allow an attacker with network access to gain administrative access without authentication. Similarly, CVE-2022-31686 is described as a broken authentication method vulnerability, and CVE-2022-31687 is a broken access control issue.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-31685	VMware Workspace ONE Assist versions 21.03 to 22.04	cpe:2.3:a:vmware:workspace_one_assist:*:*:*:*:*:*:*:*	CWE-288
CVE-2022-31686			CWE-287
CVE-2022-31687			CWE-284

Recommendations

Security Leaders

Asset and vulnerability management solutions should be implemented to ensure that all internet-accessible devices are secure, patched, updated, hardened, and monitored. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize the vulnerability, identify the impacted assets, and patch them through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Patch Details' on the following pages.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	T1040 Network Sniffing
T1548 Abuse Elevation Control Mechanism	T1590 Gather Victim Network Information	T1190 Exploit Public-Facing Application	T1588 Obtain Capabilities
T1588.006 Vulnerabilities			

Patch Details

Upgrade VMware Workspace ONE Assist to 22.10

Links:
https://resources.workspaceone.com/view/kk9llj32v29bty77s536/en

https://resources.workspaceone.com/view/96kl35y9pjmyhfbdxpp3/en

https://resources.workspaceone.com/view/r6wdzxhmtd6zksdmswbp/en

References

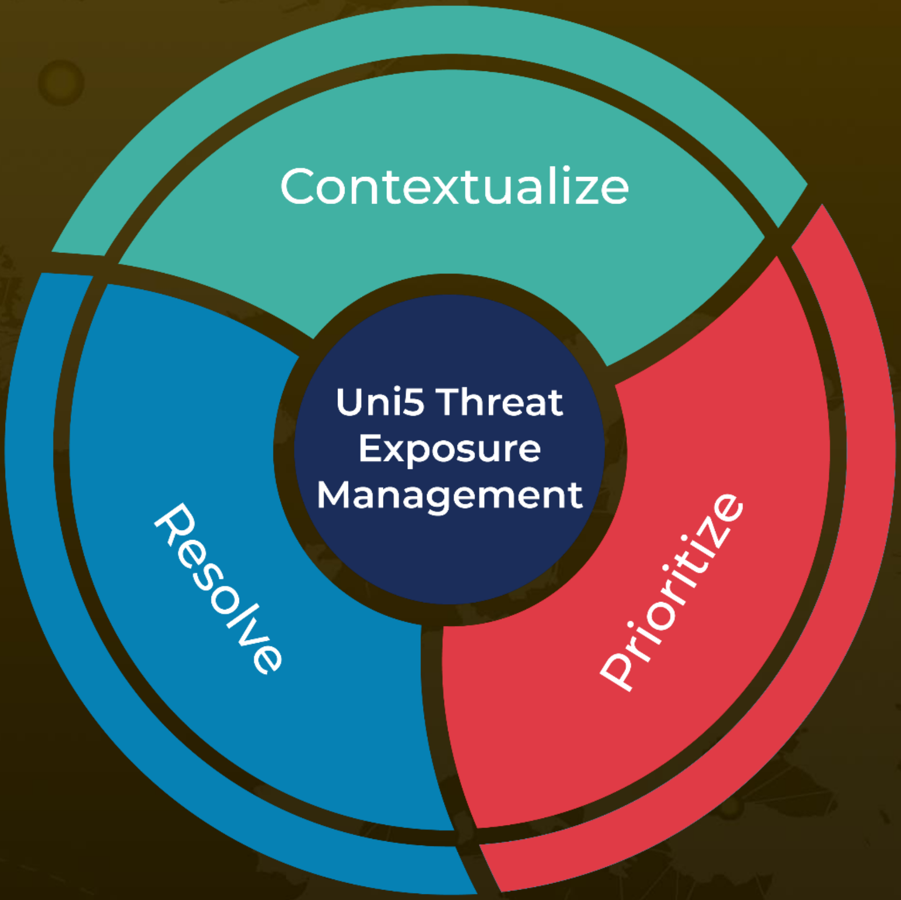
https://kb.vmware.com/s/article/89993

https://www.vmware.com/security/advisories/VMSA-2022-0028.html

What Next?

At **HivePro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **Hive Pro Uni5**: Continuous Threat Exposure Management Platform.



REPORT GENERATED ON

November 9, 2022 • 4:00 AM

More at www.hivepro.com