Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

VMware Unveils Critical Authentication Bypass Vulnerability in VCD Appliance

Date of Publication	Admiralty Code	TA Number
November 16, 2023	A1	TA2023462

Summary

First Seen: November 14, 2023
Affected Products: VMware Cloud Director Appliance (VCD Appliance)
Impact: VMware has disclosed a critical authentication bypass vulnerability affecting Cloud Director appliance deployments. This vulnerability, identified as CVE-2023-34060, the flaw could be exploited by a malicious actor to circumvent authentication protections in Cloud Director.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-34060	VMware Cloud Director Authentication Bypass Vulnerability	VMware Cloud Director Appliance (VCD Appliance)	✓	☒	☒

Vulnerability Details

#1

VMware has issued a warning about a critical security flaw, identified as CVE-2023-34060, in Cloud Director. This vulnerability could be exploited by a malicious actor to bypass authentication protections. Cloud Director is a platform that allows VMware administrators to manage cloud services within Virtual Data Centers (VDC). The flaw is specific to appliances running VCD Appliance 10.5 that were upgraded from an older release. The vulnerability does not affect fresh installations of VCD Appliance 10.5.

#2

The vulnerability arises from an error that occurred after upgrading from previous versions to version 10.5.0. Exploiting this flaw, a remote attacker can bypass login restrictions by authenticating on port 22 (ssh) or port 5480 (appliance management console), consequently gaining unauthorized access to the appliance.

#3 To address the CVE-2023-34060 in Cloud Director, VMware has provided administrators with a temporary fix until an official patch is released. The temporary solution involves downloading a custom script provided by VMware and running it on affected cells. It's important to note that this remedy is specifically designed for instances running VCD Appliance 10.5.0 that have been impacted by the vulnerability. This issue doesn't impact Linux installations.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-34060	VMware Cloud Director: 10.5.0	cpe:2.3:a:vmware:vCloud_Director:10.5.0:*:*:*:*:*:*:*	CWE-287

Recommendations

Follow Workarounds: Until an official patch is released by VMware follow the workarounds which will mitigate the CVE-2023-34060.

Limit Service Exposure: Consider limiting VCD Appliance service exposure especially SSH and appliance management console to specific trusted networks to reduce the attack surface and minimize service exposure to potential threats.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0004** Privilege Escalation	**TA0006** Credential Access
T1588 Obtain Capabilities	**T1588.006** Vulnerabilities	**T1078** Valid Accounts	**T1190** Exploit Public-Facing Application
T1556 Modify Authentication Process			

Workarounds

Vmware has provided a temporary fix until an official patch is released. The remedy involves downloading and running a custom script on affected cells running VMware Cloud Director 10.5.0. The following command can be executed to verify if your cell is exposed to the vulnerability.
egrep 'unknown|sufficient|use_first_pass|optional pam_sss' /etc/pam.d/system*

Link:
https://kb.vmware.com/s/article/95534

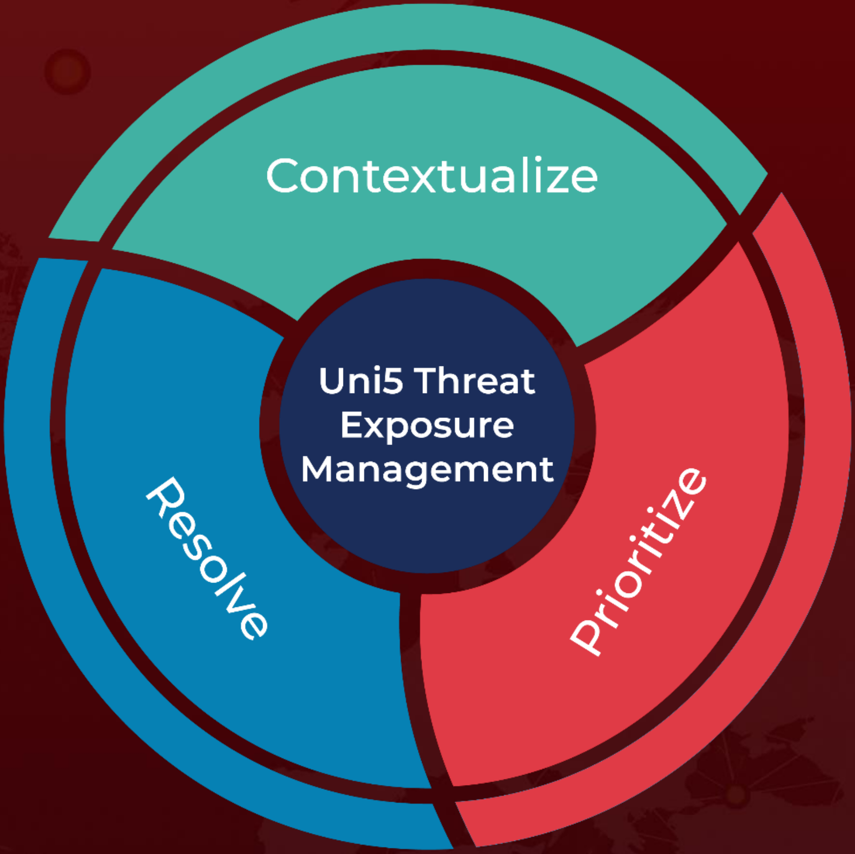
References

https://www.vmware.com/security/advisories/VMSA-2023-0026.html

What Next?

At **Hive Pro**, 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 **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

November 16, 2023 • 4:45 AM

More at www.hivepro.com