

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Injection vulnerability in VMware Carbon Black App Control

Date of Publication

February 22, 2023

Admiralty Code

A1

TA Number

TA2023096


Summary

First Seen: February 21, 2023

Affected Product: VMware Carbon Black App Control (App Control)

Impact: An injection vulnerability occurs as a result of manipulating an unknown input.

CVE

CVE	NAME	PATCH
CVE-2023-20858	Injection Vulnerability	

Vulnerability Details

There is an injection vulnerability in VMware, specifically in the Carbon Black App Control product. If a malicious actor, who has privileged access to the App Control administration console, utilizes specially crafted input, they might be able to gain access to the underlying server.

Vulnerability

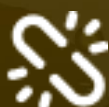
CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-20858	VMware Carbon Black App Control Server: 8.7 - 8.9.3	cpe:2.3:a:vmware:carbon_black_app_control_server:*:*:*:*:*:*:*	CWE-94

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

<u>TA0001</u> Initial Access	<u>TA0042</u> Resource Development	<u>TA0004</u> Privilege Escalation	<u>TA0005</u> Defense Evasion
<u>T1588</u> Obtain Capabilities	<u>T1588.006</u> Vulnerabilities	<u>T1055</u> Process Injection	<u>T1190</u> Exploit Public-Facing Application

Patch Details

<https://docs.vmware.com/en/VMware-Carbon-Black-App-Control/services/cb-ac-announcements/GUID-7464A525-BCF4-4329-9228-B040C9C16D22.html>

<https://docs.vmware.com/en/VMware-Carbon-Black-App-Control/services/cb-ac-announcements/GUID-35DA49E4-41F3-485B-88E5-AE69B354F2FB.html>

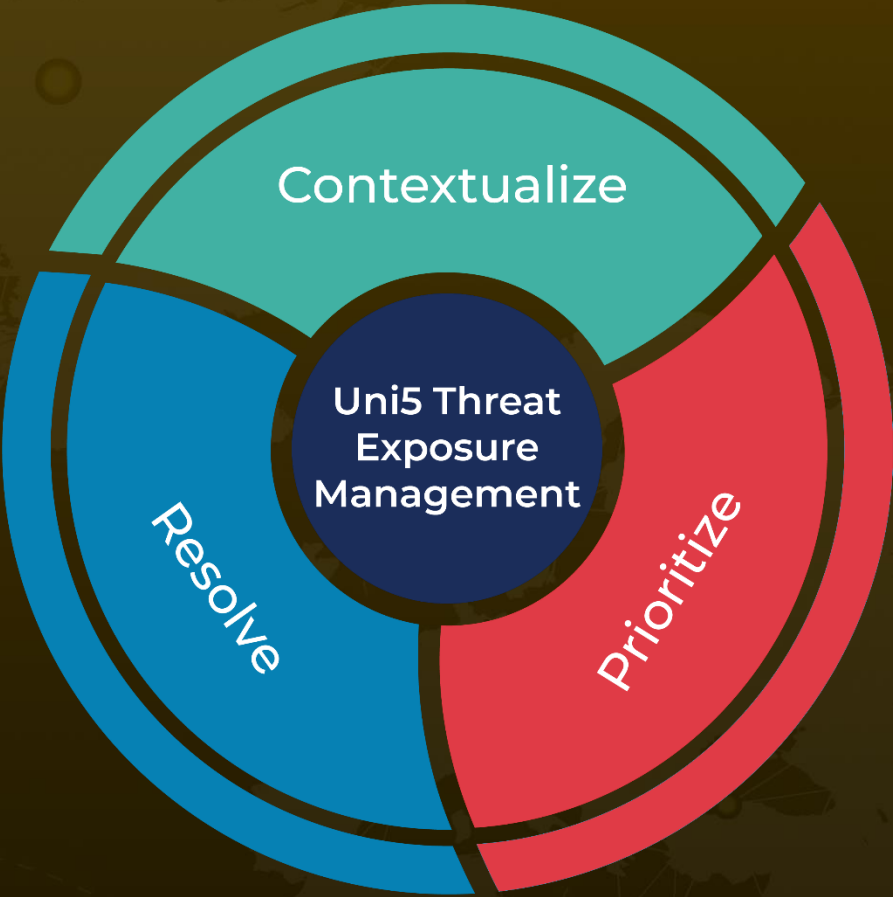
References

<https://www.vmware.com/security/advisories/VMSA-2023-0004.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

February 22, 2023 • 1:00 AM

© 2023 All Rights are Reserved by HivePro



More at www.hivepro.com