

CTI Threat Bulletin

VMware Carbon Black App Control Authentication Bypass

Executive Summary

On June 23, 2021 VMware released security bulletin [VMSA-2021-0012](#): A vulnerability in the VMware Carbon Black App Control management server could allow for an attacker to bypass authentication and obtain administrative access to the product.

Description

A vulnerability has been found in the VMware Carbon Black App Control Management Server. If given Network access to the server, an attacker could obtain administrative access to the product without the need to authenticate.

Affected Products

- AppC 8.6.x, 8.5.x, 8.1.x, 8.0.x

Safeguards/Recommendations

Affected customers are advised update AppC versions 8.6.x, and 8.5.x to versions 8.6.2, and 8.5.8 respectively. Customers using versions 8.1.x and 8.0.x are advised to apply the given [Hotfix](#).

References

<https://www.vmware.com/security/advisories/VMSA-2021-0012.html>

<https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L>

Version History

Version 1. Initial Report



Vendor: VMware

CVE-ID: CVE-2021-21998

Published: June 22, 2021

CVSS V3 Overall score: 9.4

Criticality: Critical

Patch Availability: Yes

Vulnerability Type:
Exploit Public-Facing Application

Exploitability Metrics

Attack Vector: Network

Attack Complexity: Low

Privileges Required: None

User Interaction: None

Impact Metrics

Scope: Unchanged

Confidentiality: High

Integrity: High

Availability: Low

Confidence Metrics

Exploitability: Not Defined

Remediation Level: Not Defined

Report Confidence: Not Defined



Contact Us

24x7 SOC Phone: 215.867.9051

Email: soc@sra.io

Website: <https://sra.io>