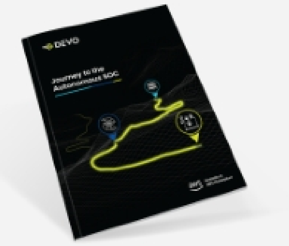

VULNERABILITIES

VMware Plugs Critical Carbon Black App Control Flaw

VMware issues a critical fix for a vulnerability that allows hacker to gain full access to the underlying server operating system.

By Ryan Naraine
February 21, 2023

Virtualization technology giant VMware on Tuesday pushed out

TRENDING

1 AI Helps Crack NIST-Recommended Post-Quantum Encryption Algorithm

2 Apple Updates Advisories as Security Firm Discloses New Class of Vulnerabilities

3 Fortinet Patches Critical Code Execution Vulnerabilities in FortiNAC, FortiWeb

a major security fix to cover a critical vulnerability in its enterprise-facing Carbon Black App Control product.

A critical-severity advisory from VMware tracks the vulnerability as CVE-2023-20858 and warns that hackers can launch injection exploits to gain full access to the underlying server operating system.

“A malicious actor with privileged access to the App Control administration console may be able to use specially crafted input allowing access to the underlying server operating system,” VMware warned.

The vulnerability, which carries a CVSS severity score of 9.1 out of 10, affects App Control versions 8.7.x, 8.8.x and 8.9.x running on Microsoft’s Windows operating system.

The company said the issue was privately reported by Jari Jääskelä, a security researcher active on the HackerOne bug bounty platform.

VMware Carbon Black App Control is a security product used by enterprise defenders to ensure that only trusted and approved software is allowed to execute on critical systems and endpoints.

VMware also issued an important-severity advisory to warn of a privilege escalation and information disclosure flaw in its vRealize Orchestrator product.

"A malicious actor, with non-administrative access to vRealize Orchestrator, may be able to use specially crafted input to bypass XML parsing restrictions leading to access to sensitive information or possible escalation of privileges," the company said.

Related: Gaping Authentication Bypass Holes in VMware Workspace One

Related: VMware Says No Evidence of Zero-Day Exploits in ESXi Ransomware Attacks

Related: VMware Patches VM Escape Flaw Exploited at Geekpwn Event

WRITTEN BY

Ryan Naraine

Ryan Naraine is Editor-at-Large at SecurityWeek and host of the

EXPERT INSIGHTS

Enterprise Blind Spots and Obsolete Tools – Security Teams Must Evolve

The conventional tools we rely on to defend corporate networks are creating gaps in network visibility and in our capabilities to secure them. (Matt Wilson)