Security Advisory 2022-020

Multiple Critical Vulnerabilities in VMware Carbon Black

March 25, 2022 — v1.0

TLP:WHITE

History:

- *25/03/2022 — v1.0 – Initial publication*

Summary

On 23/03/2022, VMware has published multiple critical vulnerabilities (`CVE-2022-22951` , `CVE-2022-22952`) [2, 3] in VMware products which allow remote code execution. These vulnerabilities may lead to gaining control over the targeted system. Both vulnerabilities rated with CVSSv3 base score of 9.1 out of 10. [1]

Technical Details

VMware Carbon Black App Control (AppC) contains an OS command injection vulnerability (`CVE-2022-22951`) and a file upload vulnerability (`CVE-2022-22952`).

According to VMware, the `CVE-2022-22951` [2] is an OS command injection vulnerability which allows an **authenticated, high privileged** malicious actor with network access to the VMware App Control administration interface to execute commands on the server due to improper input validation leading to remote code execution.

Additionally, the `CVE-2022-22952` [3] is related to a file upload vulnerability which allows a malicious actor with **administrative access** to the VMware App Control administration interface to execute code on the Windows instance where AppC Server is installed by uploading a specially crafted file.

Affected Products

Below is the list of the affected products which are running on Windows:

- VMware Carbon Black App Control versions 8.8.x
- VMware Carbon Black App Control versions 8.7.x
- VMware Carbon Black App Control versions 8.6.x
- VMware Carbon Black App Control versions 8.5.x

Recommendations and Workarounds

CERT-EU recommends following the specific steps listed for each of the following version of the product to address the reported issue.

Patches are available for each of the affected versions on VMware website. [1]

There is no known workaround for the reported vulnerabilities.

References

[1] https://www.vmware.com/security/advisories/VMSA-2022-0008.html

[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22951

[3] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22952