Critical Vulnerability in Vmware Product

June 24, 2021 — v1.0

TLP:WHITE

History:

- *24/06/2021 — v1.0 – Initial publication*

Summary

On 22nd of June 2021, VmWare released an advisory to address an authentication bypass vulnerability in VMware Carbon Black App Control (AppC). Severity of this vulnerability is **critical** with a CVSSv3.1 Base Score: 9.4 [1].

Technical Details

The VMware Carbon Black App Control management server has an authentication bypass. A malicious actor with network access to the VMware Carbon Black App Control management server might be able to obtain administrative access to the product without the need to authenticate [1].

The vulnerability is identified as CVE-2021-21998 [2].

Products Affected

VMware Carbon Black App Control (AppC) versions [1]:

- 8.6.x (fixed in 8.6.2),
- 8.5.x (fixed in 8.5.8),
- 8.1.x, 8.0.x (fixed only through a Hotfix)

Recommendations

CERT-EU recommends updating the vulnerable application as soon as possible using the patches listed in [1].

Workarounds and Mitigations

There are no workarounds announced for this vulnerability.

References

[1] https://www.vmware.com/security/advisories/VMSA-2021-0012.html

[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21998