10 years CERT-EU

Security Advisory 2023-014

Critical Vulnerabilities in VMware Products

February 23, 2023 — v1.0

TLP:CLEAR

History:

- *23/02/2023 — v1.0 – Initial publication*

Summary

On February 21, 2023, VMware released several advisories regarding critical vulnerabilities affecting Carbon Black App Control and VMware vRealize tools. The first vulnerability is identified as `CVE-2023-20858` (CVSSv3 score of 9.1) and impacts several versions of Carbon Black App Control for Windows. The second vulnerability is identified as `CVE-2023-20855` (CVSSv3 score of 8.8) and impacts VMware vRealize tools and VMware Cloud Foundation.

Technical Details

CVE-2023-20858:

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. Injection flaws allow attackers to execute commands or code in the target app, and they could lead to a complete compromise of back-end systems and all clients that connect to the vulnerable application [1,2].

CVE-2023-20855:

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 [4].

Affected Products

The `CVE-2023-20858` impacts VMware Carbon Black App Control for Windows versions [1]:

- VMware Carbon Black App Control for Windows versions 8.7.x;
- VMware Carbon Black App Control for Windows versions 8.8.x;
- VMware Carbon Black App Control for Windows versions 8.9.x.

The `CVE-2023-20855` impacts [4]:

- VMware vRealize Orchestrator running on virtual appliances versions 8.x;

- VMware vRealize Automation versions 8.x;
- VMware Cloud Foundation version 4.x.

Recommendations

CERT-EU recommends updating:

- the VMware Carbon Black App Control to fixed versions accordingly [1]:
  - 8.7.8;
  - 8.8.6;
  - 8.9.4.
- the VMware vRealize Orchestrator and Automation to the fixed version 8.11.1 [4];
- the VMware Cloud Foundation to the fixed version [4].

References

[1] https://www.vmware.com/security/advisories/VMSA-2023-0004.html

[2] https://www.bleepingcomputer.com/news/security/vmware-warns-admins-of-critical-carbon-black-app-control-flaw/

[3] https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmwcb-datasheet-app-control.pdf

[4] https://www.vmware.com/security/advisories/VMSA-2023-0005.html