Security Advisory 2023-084

Critical Vulnerability in VMware products

October 27, 2023 — v1.0

TLP:CLEAR

History:
- 27/10/2023 — v1.0 – Initial publication

Summary

On 25 October 2023, VMware has released security updates to address two vulnerabilities affecting vCenter Server and Cloud Foundation. The exploitation of the vulnerabilities could lead to an out-of-bounds write and a partial information disclosure. The vulnerabilities are tracked as CVE-2023-34048 with a CVSS score 9.8 and CVE-2023-34056 with a CVSS score of 4.3.[1] It is recommended updating as soon as possible.

Technical Details

- **CVE-2023-34048**: This vulnerability (CVSS score of 9.8) allows a malicious actor with network access to vCenter Server to trigger an out-of-bounds write potentially leading to remote code execution.
- **CVE-2023-34056**: This vulnerability (CVSS score of 4.3) allows a malicious actor with non-administrative privileges to vCenter Server to leverage this issue to access unauthorised data.

Affected products

- VMware vCenter Server versions 7.x and 8.x;
- VMware Cloud Foundation (VMware vCenter Server) versions 4.x and 5.x.

Recommendations

CERT-EU recommends updating affected software to the latest version as soon as possible.
References