Security Advisory 2024-060

Vulnerabilities in VMware Products

June 18, 2024 — v1.0

TLP:CLEAR

History:
- 18/06/2024 — v1.0 – Initial publication

Summary

On June 17, 2024, VMware released fixes for three vulnerabilities affecting VMware vCenter Server and VMware Cloud Foundation. Two of these vulnerabilities are critical. Exploitation these vulnerabilities could allow a malicious actor to execute remote code or escalate privileges on the affected systems [1].

Technical Details

The vulnerabilities CVE-2024-37079 and CVE-2024-37080, both with a CVSS score of 9.8, are heap-overflow vulnerabilities in the DCERPC protocol implementation. An attacker with network access to vCenter Server can exploit these vulnerabilities to execute remote code by sending a specially crafted network packet.

The vulnerability CVE-2024-37081, with a CVSS score of 7.8, is a local privilege escalation vulnerability caused by sudo misconfiguration. An authenticated local user with non-administrative privileges can exploit this vulnerability to gain root privileges.

Affected Products

These vulnerabilities affect VMware vCenter Server 7.0 and 8.0, and VMware Cloud Foundation 4.x and 5.x [1].

Recommendations

CERT-EU strongly recommends updating affected software to the latest versions by following the instructions given by the vendor.
References

[1] https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24453