CERT-EU

Security Advisory 2024-100

Critical RCE Vulnerability in VMware vCenter Server

October 22, 2024 — v1.1

TLP:CLEAR

History:

- *18/09/2024 — v1.0 – Initial publication*
- *22/10/2024 — v1.1 – Update about an incomplete patch*

Summary

On September 17, 2024, Broadcom released a fix for a critical vulnerability tracked as **CVE-2024-38812** in VMware vCenter Server, enabling remote code execution (RCE) via a specially crafted network packet [1]. Following this, on October 21, 2024, Broadcom updated their advisory [2] with additional information about another related vulnerability tracked as **CVE-2024-38813**.

Technical Details

- The critical vulnerability **CVE-2024-38812** is caused by a heap overflow in vCenter Server's DCE/RPC protocol implementation. This allows an unauthenticated attacker to remotely execute arbitrary code without user interaction.
- Another high-severity vulnerability, **CVE-2024-38813**, enables privilege escalation to root via specially crafted network packets.

Affected Products

The following products are affected:

- VMware vCenter Server 7.0 (fixed in 7.0 U3s) and 8.0 (fixed in 8.0 U3b)
- VMware Cloud Foundation 4.x (fixed in async patch to 7.0 U3s) and 5.x (fixed in async patch to 8.0 U3b)

Recommendations

CERT-EU recommends to apply the available patches via the VMware Security Advisory [2].

The VCenter patches released on September 17, 2024 did not completely address CVE-2024-38812. The patches listed in [2] are updated versions that contain additional fixes to fully address CVE-2024-38812.

References

[1] https://www.bleepingcomputer.com/news/security/broadcom-fixes-critical-rce-bug-in-vmware-vcenter-server/

[2] https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24968