CERT-EU

Security Advisory 2022-036

# Critical Vulnerabilities in VMware Products

*May 25, 2022 — v1.1*

**TLP:WHITE**

*History:*

- *18/05/2022 — v1.0 – Initial publication*
- *25/05/2022 — v1.1 – Update following a POC release*

## Summary

On the 18th of May 2022, VMware released an advisory about two critical vulnerabilities. Tracked as CVE-2022-22972 and CVE-2022-22973 with a respective CVSS score of 9.8 and 7.8, a successful exploitation of these vulnerabilities allows an **unauthenticated** attacker to achieve an **authentication bypass** affecting local domain users and a **privilege escalation** gaining `root` access [1].

On the 25th of May 2022, security researchers at attack surface assessment company Horizon3 announced that they managed to create a working proof-of-concept (PoC) exploit code for CVE-2022-22972 and will likely release a technical report at the end of the week. No technical details have been released yet, but the plan includes publishing exploit code that demonstrates the attack vector [2].

It is **strongly** recommended to apply the patches as soon as possible.

## Technical Details

The `CVE-2022-22972` (Authentication Bypass) affects local domain users. It impacts VMware Workspace ONE Access, Identity Manager and vRealize Automation. In order to exploit this vulnerability, a remote attacker capable of accessing the respective user interface could bypass the authentication for these various products.

The `CVE-2022-22973` is a local privilege escalation vulnerability in the VMware Workspace ONE Access and Identity Manager. In order to exploit this vulnerability, an attacker would need to have local access to the vulnerable instances of Workspace ONE Access and Identity Manager. Successful exploitation would allow an attacker to gain `root` privileges [3].

## Affected Products

Affected products include:

- VMware Workspace ONE Access (Access)
- VMware Identity Manager (vIDM)
- vRealize Lifecycle Manager
- VMware vRealize Automation (vRA)
- VMware Cloud Foundation

To see more about the impacted versions, please refer directly to the response matrix in the VMware advisory [1].

## Recommendations and Workarounds

CERT-EU strongly recommends to apply the vendor patch(es) as soon as possible [4].

Detailed instructions with workarounds are available by VMware for specific versions of the affected product in case the patch(es) cannot be applied immediatly [5].

## References


[1] https://www.vmware.com/security/advisories/VMSA-2022-0014.html

[2] https://www.bleepingcomputer.com/news/security/researchers-to-release-exploit-for-new-vmware-auth-bypass-patch-now/

[3] https://www.tenable.com/blog/cve-2022-22972-vmware-patches-additional-workspace-one-access-vulnerabilities-vmsa-2022-0014

[4] https://kb.vmware.com/s/article/88438

[5] https://kb.vmware.com/s/article/88433