CERT-EU

Security Advisory 2022-025

Critical Vulnerabilities in VMware

May 24, 2022 — v1.1

TLP:WHITE

History:

- *07/04/2022 — v1.0 – Initial publication*
- *24/05/2022 — v1.1 – Updated with information about active exploitation*

Summary

On April 6th, VMware released several security patches for critical-severity flaws affecting multiple products. The vulnerabilities identified as `CVE-2022-22954`, `CVE-2022-22955`, `CVE-2022-22956`, `CVE-2022-22957`, and `CVE-2022-22958` can lead to multiple effects such as remote code execution and authentication bypass.

VMware also patched high and medium severity bugs that could be exploited for Cross-Site Request Forgery (CSRF) attacks (`CVE-2022-22959`), privilege escalation (`CVE-2022-22960`), and gain access to information without authorisation (`CVE-2022-22961`) [1].

On May 20th, Unit 42 has observed numerous instances of `CVE-2022-22954` being exploited in the wild [4]. When successful, `CVE-2022-22960` can be leveraged to run commands as a root user. It is strongly recommended to patch as soon as possible [2].

Technical Details

Here are the technical details of the vulnerabilities :

- `CVE-2022-22954` - CVSS score: 9.8 - VMware Workspace ONE Access and Identity Manager contain a remote code execution vulnerability due to server-side template injection.
- `CVE-2022-22955` and `CVE-2022-22956` - CVSS score: 9.8 - VMware Workspace ONE Access has two authentication bypass vulnerabilities in the OAuth2 ACS framework.
- `CVE-2022-22957` and `CVE-2022-22958` - CVSS score: 9.1 - VMware Workspace ONE Access, Identity Manager and vRealize Automation contain two remote code execution vulnerabilities.
- `CVE-2022-22959` - CVSS score: 8.8 - VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a cross site request forgery vulnerability.
- `CVE-2022-22960` - CVSS score: 7.8 - VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a privilege escalation vulnerability due to improper permissions in support scripts.

- `CVE-2022-22961` - CVSS score: 5.3 - VMware Workspace ONE Access, Identity Manager and vRealize Automation contain an information disclosure vulnerability due to returning excess information.

Affected Products

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

Recommendations and Workarounds

CERT-EU recommends to apply the patches or the workarounds provided by VMware [2]. While applying workarounds is possible, VMware strongly recommends patching as the simplest and most reliable way to resolve this issue.

VMware has also published a document with additional questions and answers regarding VMSA-2021-0011 [3].

Since vulnerabilities `CVE-2022-22954` and `CVE-2022-22960` are exploited in the wild [4], it is highly recommended to apply the patches as soon as possible.

References

[1] https://www.bleepingcomputer.com/news/security/vmware-warns-of-critical-vulnerabilities-in-multiple-products/

[2] https://www.vmware.com/security/advisories/VMSA-2022-0011.html

[3] https://core.vmware.com/vmsa-2022-0011-questions-answers-faq

[4] https://unit42.paloaltonetworks.com/cve-2022-22954-vmware-vulnerabilities/