Security Advisory 2022-057

Critical Vulnerability in VMware Products

August 3, 2022 — v1.0

TLP:WHITE

History:

- *02/08/2022 — v1.0 – Initial publication*

Summary

On August 2, 2022, multiple critical vulnerabilities were reported by VMware. Exploitation of these vulnerabilities may lead to an unauthenticated remote code execution on the affected servers. [1]

Technical Details

This advisory contains multiple vulnerabilities with high severity that may be chained.

- **CVE-2022-31656**: Authentication bypass.

This vulnerability, with a CVSS score of 9.8 out of 10, could allow an unauthenticated user with network access to the WMware Workspace ONE Access, Identity Manager and vRealize Automation to gain administrative access on these platforms.

- **CVE-2022-31658, CVE-2022-31665**: JDBC Injection Remote Code Execution Vulnerability

These vulnerabilities, with a severity score of, respectively, 8.0 and 7.6 out of 10, may allow a user with administrative rights and network access to WMware Workspace ONE Access, Identity Manager and vRealize Automation to trigger a remote code execution via a JDBC injection on these platforms.

- **CVE-2022-31659**: SQL injection Remote Code Execution Vulnerability

This vulnerability, with a CVSS score of 8.0 out of 10, could allow a user with administrative rights and network access to WMware Workspace ONE Access, Identity Manager and vRealize Automation to trigger a remote code execution via an SQL injection on these platforms.

- **CVE-2022-31660, CVE-2022-31661, CVE-2022-31664**: Local privilege escalation.

These vulnerabilities, with a CVSS score of 7.8 out of 10 each, could allow a user with local access to VMware Workspace ONE Access, Identity Manager and vRealize Automation to escalate privileges to `root`.

Three lower vulnerabilities including a URL injection (CVE-2022-31657), a path traversal (CVE-2022-31662) and an XSS vulnerability (CVE-2022-31663) are also reported affecting these products.

Products Affected

The following products are impacted:

- VMware Workspace ONE Access (Access) - 21.08.0.1, 21.08.0.0
- VMware Identity Manager (vIDM) - 3.3.4, 3.3.5, 3.3.6
- VMware Identity Manager Connector (vIDM Connector) - 3.3.4, 3.3.5, 3.3.6
- VMware vRealize Automation (vRA) - 7.6 and 8.x (if deployed with vIDM)
- VMware Cloud Foundation (deploy vIDM) - 4.4.x, 4.3.x, 4.2.x
- VMware Cloud Foundation (deploy vRA) - 3.x
- vRealize Suite Lifecycle Manager (deploy vIDM) - 8.x

A complete Reponse Matrix is available on the VMware security advisory [2].

Recommendations

CERT-EU strongly recommends upgrading the affected products to the last available version. When patching is not possible, CERT-EU strongly recommends applying the workaround provided by VMWare. [3,4]

References

[1] https://www.bleepingcomputer.com/news/security/vmware-urges-admins-to-patch-critical-auth-bypass-bug-immediately/

[2] https://www.vmware.com/security/advisories/VMSA-2022-0021.html

[3] https://kb.vmware.com/s/article/89096

[4] https://kb.vmware.com/s/article/89084