

Security Advisory 2023-040

Multiple Vulnerabilities in VMWare Products

June 23, 2023 — v1.0

TLP:CLEAR

History:

- 23/06/2023 — v1.0 – Initial publication

Summary

On June 22, VMWare released an advisory regarding multiple memory corruption high severity vulnerabilities in VMware vCenter Server. The affected software provides a centralised and extensible platform for managing virtual infrastructure [1,2]. The vulnerabilities were found in the DCERPC protocol implementation utilised by vCenter Server. The protocol allows for smooth operation across multiple systems by creating a virtual unified computing environment [3].

Technical Details

- [CVE-2023-20892](#) (CVSSv3 base score of 8.1) - a heap overflow vulnerability due to the usage of uninitialised memory in the implementation of the DCERPC protocol. A malicious actor with network access to vCenter Server may exploit this issue to execute arbitrary code on the underlying operating system that hosts vCenter Server.
- [CVE-2023-20893](#) (CVSSv3 base score of 8.1) - a use-after-free vulnerability in the implementation of the DCERPC protocol. A malicious actor with network access to vCenter Server may trigger an out-of-bounds write vulnerability in the implementation of the DCERPC protocol. A malicious actor with network access to vCenter Server may trigger an out-of-bound write by sending a specially crafted packet leading to memory corruption.
- [CVE-2023-20895](#) (CVSSv3 base score of 8.1) - a memory corruption vulnerability in the implementation of the DCERPC protocol. A malicious actor with network access to vCenter Server may trigger a memory corruption vulnerability which may bypass authentication.

Affected Products

- vCenter Server 7.0 [1]
- vCenter Server 8.0 [1]
- Cloud Foundation (vCenter Server) 4.x [1]
- Cloud Foundation (vCenter Server) 5.x [1]

Recommendations

CERT-EU highly recommends installing the fixed versions as soon as possible:

- vCenter Server 7.0 U3m [1]
- vCenter Server 8.0 U1b [1]
- Cloud Foundation (vCenter Server) 7.0 U3m [1]
- Cloud Foundation (vCenter Server) 8.0 U1b [1]

References

[1] <https://www.vmware.com/security/advisories/VMSA-2023-0014.html>

[2] <https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/vCenter/vmware-vcserver-datasheet.pdf>

[3] <https://vulnera.com/newswire/vmware-addresses-high-severity-security-flaws-in-vcserver/>