CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2020-021

Critical Vulnerability in VMware vCenter

April 11, 2020 — v1.0

TLP:WHITE

History:

- *11/04/2020 — v1.0 – Initial publication*

Summary

On April 9, 2020, VMware vCenter Server updates were issued, which address sensitive information disclosure vulnerability in the VMware Directory Service `vmdir` (CVE-2020-3952) [1]. A malicious actor with network access to an affected deployment may be able to extract highly sensitive information which could be used to compromise vCenter Server or other services. VMware has evaluated the severity of this issue to be in the Critical severity range with a maximum CVSSv3 base score of 10.0.

Technical Details

A sensitive information disclosure vulnerability in the VMware Directory Service `vmdir` has been discovered [1]. Under certain conditions `vmdir` that ships with VMware vCenter Server does not correctly implement access controls.

A malicious actor with network access to an affected `vmdir` deployment may be able to extract highly sensitive information which could be used to compromise vCenter Server or other services which are dependent upon `vmdir` for authentication.

Products Affected

VMware vCenter Server 6.7 (embedded or external PSC) prior to 6.7u3f is affected, **if it was upgraded from a previous release line** such as 6.0 or 6.5 [2].

VMware vCenter versions 6.5 and 7.0, as well as **clean installations of vCenter Server 6.7** (embedded or external PSC) **are not affected** [1].

Recommendations

Check if your installation is affected by following steps in [2].

If necessary, upgrade to your vCenter Server installation to version 6.7u3f [3].

References

[1] https://www.vmware.com/be/security/advisories/VMSA-2020-0006.html

[2] https://kb.vmware.com/s/article/78543

[3] https://my.vmware.com/web/VMware/details?productId=742&rPId=44888&downloadGroup=VC67U3F