VMWare Directory Service Critical Vulnerability

A highly critical vulnerability was detected in VMWare's Directory Service product, specifically version 6.7 installations that were upgraded from versions 6.0 and 6.5[i]. VMWare server virtualization systems enable the virtualization and consolidation of many traditionally physical computer systems, which Healthcare and Public Health (HPH) entities may be using to support much of their IT infrastructure. VMWare's Directory Service product is a central component element of Single Sign-On services (SSO) in VMware's vCenter Server product[ii]. Exploiting this vulnerability, a malicious actor with network access may be able to extract highly sensitive information and bypass other authentication mechanisms[iii]. Recommended actions are to upgrade affected deployments to newer versions (i.e., versions 6.7u3f or 7.0).

VMware Securities Advisories (VMSA) published an advisory document VMSA-2020-0006 on 9 April, 2020. This document identified a critical information disclosure vulnerability, CVE-2020-3952. This vulnerability focuses on VMware Directory Service (vmdir). The vmdir is part of VMware's vCenter Server product, which provides centralized management of virtualized hosts and virtual machines (VMs) from a single console. Under certain conditions, vmdir does not implement proper access controls[iv & v]. VMware evaluated the severity of this issue to be in the critical severity range with a maximum CVSSv3 base score of 10 out of 10.

The vulnerability only affects vCenter Server version 6.7 instances upgraded from versions 6.0 or 6.5. Clean installs of vCenter Server 6.7 (embedded or external PSC) are not affected.

Recommended actions

- Review system log files to determine if an implementation of VMWare's Directory Service is affected.
  - Affected deployments will create a log entry when the vmdir service starts stating that legacy ACL mode is enabled.
- Upgrade affected systems to VMWare Directory Service version 6.7u3f or 7.0.

[i] VMware. (April 9 2020). VMware Security Advisories. vmware.com. Accessed 14 April 2020 at https://www.vmware.com/security/advisories/VMSA-2020-0006.html

[ii] VMware. (May 31 2019). vCenter Single Sign-On Components. VMware.com. Accessed 14 April at https://docs.vmware.com/en/VMware-vSphere/6.0/com.vmware.vsphere.install.doc/GUID-90C1E3DC-4397-4BF0-808E-DF3802E56BC6.html

[iii] Paganini, P. (April 10 2020). CVE-2020-3952 flaw could allow attackers to hack VMware vCenter Server. Accessed14 April 2020 at https://securityaffairs.co/wordpress/101388/security/cve-2020-3952-vmware-vcenter-server.html

[iv] Seals, T.(April 10 2020). Critical VMware Bug Opens Up Corporate Treasure to Hackers. Accessed 14 April 2020 at https://threatpost.com/critical-vmware-bug-corporate-treasure-hackers/154682/

[v] Olenick, D. (April 13 2020). VMware issues 10.0 CVSS rating on vCenter Server vulnerability. Accessed 14 April 2020, at https://www.scmagazine.com/home/security-news/vulnerabilities/vmware-issues-10-0-cvss-rating-on-vcenter-server-vulnerability/