July 08, 2024, **CYBERSECURITY**

Topic: VMware ESXi Multiple Vulnerabilities

Overview:

Several vulnerabilities, based on the VMWare operating systems ESXi, have been published by the supplier VMWare in their security bulletins:

- **VMSA-2024-0011 (23/05/2024):**
  https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24308

- **VMSA-2024-0013 (26/06/2024):**
  https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24505

Arabelle Solutions has identified several products that include an impacted VMWare ESXi version, listed below:

Affected Versions:

- VMware ESXi: Versions 7.0
- VMware ESXi: Versions 8.0

Impacted Products:

- Mark VIe OT Armor Security
- Cyber Jump Station (Secure Remote Connection)
- Cyber Alspa Security Server
- Alspa Virtualisation Server
- Digital Product KPE Server

Identified risks:

CVE-2024-22273 - Vulnerability Details – Out-of-bounds read/write vulnerability
CVSSv3 Score: 8.1 (High)
A malicious actor with access to a virtual machine with storage controllers enabled may exploit this issue to create a denial-of-service condition or execute code on the hypervisor from a virtual machine in conjunction with other issues.

CVE-2024-37086 - Vulnerability Details – VMWare ESXi out-of-bounds read vulnerability
CVSSv3 Score: 6.8 (Medium)
A malicious actor with local administrative privileges on a virtual machine with an existing snapshot may trigger an out-of-bounds read leading to a denial-of-service condition of the host.

Mitigation:
There is no specific mitigation or workaround given by the supplier VMWare to cover CVE-2024-22273.
To cover CVE-2024-37086, a mitigation could consist by the removing all existing snapshots and not store any snapshot on the asset.

Remediation:
The solution given by the supplier is the upgrade of the product:

Product	Version	Fixed Version
ESXi	7.0	**ESXi70U3sq-23794019 (7.0 Update 3q)**
ESXi	8.0	**ESXi80U3-24022510 (8.0 Update 3)**

Reminder:
Some basic rules must be put in place about access to virtual machines. Physically, the server host must be:

- in a room with restricted and authorized access,
- in a locked cubicle with restricted access.

Moreover, following the best practices put in place for cyber, management access through ESXi must be protected by a strong password.

Defense-in-depth:
To minimize the risk of the exploitation of current and future system vulnerabilities, Arabelle Solutions highly recommends implementation of a defense-in-depth strategy (complementary defenses in Physical, Technical, and administrative domains) for your critical process control systems.

We will be pleased to support you in the enhancement of your cybersecurity strategy and improve or update your current equipment with latest cybersecurity methodologies and solutions. We suggest that a thorough analysis of your cybersecurity status be performed and resulting recommendations for an optimal solution be implemented according to the level of risk exposure and/or the standard frameworks which are applicable to your needs.

Contact your Arabelle Solutions Automation & Controls Sales person or our Help Desk at +33 1 60 13 43 91 /
helpdesk.control-systems@arabellesolutions.com for help with ordering cybersecurity services and solutions.

Revision History

Version	Release Date	Purpose
A	July 08, 2024	Initial version