MONTELEKTRO

SJEDIŠTE RIJEKA
Kudeji 53
HR-51215 Kastav
rijeka@montelektro.hr
+ 385 51 54 58 10

URED ZAGREB
Marka Marulića 5
HR-10431 Sv. Nedelja
zagreb@montelektro.hr
+ 385 1 39 09 020

SECURITY ADVISORY

VMSA-2024-0006.1 Multiple vulnerabilities in VMware ESXi, Workstation and Fusion

Revision history:

Date	Rev.	Description
13.03.2024.	1	[RGA] Initial release

MONTELEKTRO

TABLE OF CONTENTS

1. INTRODUCTION

The purpose of this document is to address critical vulnerabilities affecting VMware ESXi, Workstation Pro & Player, and Fusion products. These vulnerabilities, identified in the VMware Security Advisory (VMSA) VMSA-2024-0006.1, could potentially allow an attacker/unauthorized party to gain elevate privileged access (root and/or administrator) on a guest OS to gain access to the underlying hypervisor host machine and/or underlying network and/or memory. Given the nature of our systems, this advisory will specifically focus on ESXi systems.

Montelektro is fully aware of these vulnerabilities and understands their potential impact on our customers' environments. We remain committed to continuous monitoring of security advisories published by the vendors of the components used in our IT infrastructure and PCS solutions. We strongly advise our customers to carefully review this document and take necessary actions. If your systems are affected, consider promptly applying patches to mitigate the risks associated with these vulnerabilities.

2. IMPACT

Impacted ESXi version: ESXi 8.0, ESXi 7.0, Cloud foundation (ESXi)5.x/4.x and up. While Broadcom does not mention end-of-life products in the Security Advisories, due to the critical severity of these vulnerabilities Broadcom has made a patch available to customers with extended support for ESXi 6.7 (6.7U3u), 6.5 (6.5U3v).

2.1. CVE-2024-22252, CVE-2024-22253 - Information Disclosure and Privilege Escalation

VMware ESXi XHCI/UHCI USB controller contains use-after-free vulnerability that enables a malicious actor to gain local administrative privileges on virtual machine to execute his own code within virtual machine's VMX process that is running on host. While the exploitation is indeed contained within the VMX sandbox, limiting potential damage, it could still enable a malicious actor to gain unauthorized access to sensitive information or disrupt VM operations.

VMware has evaluated the severity of this issue to be in the Critical severity range with a maximum CVSSv3 base score of 9.3 for Workstation/Fusion and in the Important severity range with a maximum CVSSv3 base score of 8.4 for ESXi.

2.2. CVE-2024-22254 - Out-of-Bounds Write Vulnerability

VMware ESXi contains an out-of-bound write vulnerability that enables malicious actors to trigger a memory write leading within VMX to escape sandbox environment, potentially gaining an access to the host hypervisor machine. An out-of-bounds write vulnerability occurs when a program tries to write data to a memory location that's outside the intended boundaries. In CVE-2024-22254, this vulnerability likely exists within the VMX process, which manages individual virtual machines on an ESXi host. A successful exploit could allow the malicious actor to break free of this sandbox and potentially gain full access to the ESXi host, corrupt memory, gain code execution and or launch further attacks.

VMware has evaluated the severity of this issue to be in the Important severity range with a maximum CVSSv3 base score of 7.9.

2.3. CVE-2024-22255 - Information Disclosure

VMware ESXi contains a vulnerability that resides within the Universal Host Controller Interface (UHCI) USB controller that's emulated by VMware software for guest virtual machines. A malicious actor with administrative access on a guest VM might be able to exploit a flaw in how the UHCI controller handles data to leak memory. While CVE-2024-22255 doesn't directly grant a malicious actor code execution or complete system compromise, it can be a steppingstone in a larger attack. By leaking information from the VMX process memory, an attacker could potentially discover sensitive details and identify further vulnerabilities within the system.

VMware has evaluated the severity of this issue to be in the Important severity range with a maximum CVSSv3 base score of 7.1.

3. MITIGATION

Following these mitigation steps, you can significantly reduce the risk of these vulnerabilities being exploited in your environment. However, patching is the most effective and long-term solution. There are two vectors of mitigation available now for most of these CVE's - workaround and permanent patch solution.

3.1. CVE-2024-22252, CVE-2024-22253 - Information Disclosure and Privilege Escalation

Primary mitigation is to apply security patches as soon as they become available from VMware.

Alternative temporary mitigation (with limitation) is removal of all USB controllers from all virtual machines on affected ESXi host version. However, this might disrupt functionalities requiring USB access within virtual machines and this is not a permanent solution as patching is still highly recommended.

3.2. CVE-2024-22254 - Out-of-Bounds Write Vulnerability

Primary mitigation is to apply security patches as soon as they become available from VMware. These patches will address the underlying memory corruption issue and prevent exploitation.

There is no alternative mitigation currently available for this specific vulnerability. Due to its severity, patching is essential.

3.3. CVE-2024-22255 - Information Disclosure

Primary mitigation is to apply security patches as soon as they become available from VMware. These patches will address the flaw in the UHCI USB controller and prevent information leakage.

Alternative Mitigation (consider alongside patching) is to restrict administrative privileges on guest virtual machines. By limiting the malicious actor access within the guest environment, you can potentially reduce the amount of sensitive information they can exploit through this vulnerability.

4. AVAILABLE PATCHES AND WORKAROUNDS

Table 1 - Available workaround/patch per ESXi version and vulnerability

ESXi version	Vulnerability	Workaround	Patch
VMware ESXi 8.0	CVE-2024-22252 CVE-2024-22253 CVE-2024-22255	How to remove USB controllers from a Virtual Machine	VMware ESXi 8.0 Update 1d Release Notes
	CVE-2024-22254	Not available	
VMware ESXi 7.0	CVE-2024-22252 CVE-2024-22253 CVE-2024-22255	How to remove USB controllers from a Virtual Machine	VMware ESXi 7.0 Update 3p Release Notes
	CVE-2024-22254	Not available	
VMware ESXi 6.7	CVE-2024-22252 CVE-2024-22253 CVE-2024-22255	How to remove USB controllers from a Virtual Machine	VMware ESXi 6.7, Patch Release ESXi670-202403001
	CVE-2024-22254	Not available	
VMware ESXi 6.5	CVE-2024-22252 CVE-2024-22253 CVE-2024-22255	How to remove USB controllers from a Virtual Machine	VMware ESXi 6.5, Patch Release ESXi650-202403001
	CVE-2024-22254	Not available	

5. RECOMMENDATIONS

As a general security measure, Montelektro strongly recommends protecting network access to devices with appropriate mechanisms.

Our main recommendation is to install the latest VMware security patches, but there is also the possibility of applying a workaround. Applying the workaround is simpler and will take less time, but it will disable the use of USB peripherals and the system will again be exposed to vulnerability if USB peripheral support is enabled. Since currently available workaround mitigates only 3 of the 4 listed vulnerabilities, we recommend workaround only as a temporary solution in the period before patch installation.

Installing a patch or applying a workaround can affect the operation of USB peripherals. When taking steps to mitigate these vulnerabilities, special attention should be paid to systems that use USB dongle-based licenses (such as *ABCIT Soft PLC*, *Proficy iFix*, and similar) and USB devices such as USB modems. To avoid production disruption caused by the interruption of the functioning of USB peripherals, the preferred way of mitigating the vulnerability must be tested on a non-production system beforehand.

Systems supplied by Montelektro after the official patch release are already patched during the system configuration in our workshop. Systems that are part of a properly secured PCD network and are not exposed to the outside world are not at great risk of being targeted by this vulnerability.

Patch planning and administration guidelines from Montelektro PCS IT maintenance and security whitepaper should be considered during the patch deployment.

An active SLA contract can be used to check if the system is affected and support the installation of the patch or workaround on components supplied by Montelektro.

6. REFERENCES

Montelektro. (2019, July). *Process Control System – IT maintenance and security Whitepaper*. Retrieved from Montelektro Web site: https://www.montelektro.hr/wp-content/uploads/2022/07/KB1007-Process-Control-System-IT-maintenance-and-security-.pdf

VMware. (2024, March 06). *How to remove USB controllers from a Virtual Machine (96682)*. Retrieved from VMware Customer Connect: https://kb.vmware.com/s/article/96682

VMware. (2024, March 05). *VMSA-2024-0006.1 Multiple vulnerabilities in VMware ESXi, Workstation, and Fusion*. Retrieved from VMware Security Advisories: https://www.vmware.com/security/advisories/VMSA-2024-0006.html

VMware. (2024, March 05). *VMware ESXi 6.5, Patch Release ESXi650-202403001*. Retrieved from VMWare Docs: https://docs.vmware.com/en/VMware-vSphere/6.5/rn/esxi650-202403001.html

VMware. (2024, March 05). *VMware ESXi 6.7, Patch Release ESXi670-202403001*. Retrieved from VMware Docs: https://docs.vmware.com/en/VMware-vSphere/6.7/rn/esxi670-202403001.html

VMware. (2024, March 04). *VMware ESXi 7.0 Update 3p Release Notes*. Retrieved from VMware Docs: https://docs.vmware.com/en/VMware-vSphere/7.0/rn/vsphere-esxi-70u3p-release-notes/index.html

VMware. (2024, March 05). *VMware ESXi 8.0 Update 1d Release Notes*. Retrieved from VMware Docs: https://docs.vmware.com/en/VMware-vSphere/8.0/rn/vsphere-esxi-80u1d-release-notes/index.html

VMware. (2024, March 07). *VMware ESXi 8.0 Update 2b Release Notes*. Retrieved from VMware Docs: https://docs.vmware.com/en/VMware-vSphere/8.0/rn/vsphere-esxi-80u2b-release-notes/index.html