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

CVE-2021-21974 ESXi OpenSLP heap-overflow

Revision history:

Date	Rev.	Description
17.02.2023	3	[FBA] Security advisory link changed
13.02.2023.	2	[DFL] Mitigation recommendations added
10.02.2023.	1	[FBA] Initial release

MONTELEKTRO

TABLE OF CONTENTS

1. INTRODUCTION

A critical vulnerability in OpenSLP identified by CVE-2021-21974 and CVE-2021-21995 has been publicly disclosed in 2021. This vulnerability allows for remote code execution by exploiting the heap-overflow issue in OpenSLP service.

Unpatched and unprotected VMware ESXi servers around the world have been targeted over the past few days in a large-scale ransomware attack (dubbed "ESXiArgs") exploiting this vulnerability. These exploits are generally targeting ESXi hosts exposed to the outside world on port 427.

Montelektro is aware of this vulnerability and of how it could, if exploited, potentially impact our customers' environments.

Montelektro is continuously monitoring security advisories published by vendors of the components that are used in our IT infrastructure and PCS solutions.

2. MONITORED PRODUCTS

Vulnerability exposure status of Montelektro PCS relevant products confirmed by their vendors.

2.1. Affected products

Table 1 - Affected products confirmed by vendor

Vendor	Product	Security advisory
VMware	vSphere ESXi 6.5 build 17167537 and older vSphere ESXi 6.7 build 17167734 and older vSphere ESXi 7.0 build 17168206 and older	VMware Security Advisory VMSA-2021-0002 - Updated On 2021-02-23

2.2. Unaffected products

Table 2 - Not affected products confirmed by the vendor

Vendor	**Product**	**Security advisory**
VMware	vCenter Server vSphere ESXi 6.5 build 17325551 and newer vSphere ESXi 6.7 build 17499825 and newer vSphere ESXi 7.0 build 17325551 and newer	VMware Security Advisory VMSA-2021-0002 - Updated On 2021-02-23

3. AVAILABLE MITIGATIONS AND FIXES

3.1. VMware - vSphere ESXi 7.x, 6.7.x, 6.5.x

Vulnerability has been patched since following versions:

ESXi 7.0: VMware patch to address CVE-2021-21974 in ESXi 7.0

ESXi 6.7: VMware patch to address CVE-2021-21974 in ESXi 6.7

ESXi 6.5: VMware patch to address CVE-2021-21974 in ESXi 6.5

Workaround is available as well: VMware Workaround instructions to address CVE-2021-21974 in vSphere ESXi (76372).

4. MITIGATION RECOMMENDATIONS

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

Patches to mitigate the problem are already available. Workaround can also be implemented by disabling SLP service on affected systems.

Systems supplied by Montelektro after the official patch release in 2021 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. In most PCS configurations, workaround deployment can be done in a quicker manner and without affecting the production than applying the patch.

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.

5. 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

NIST. (2022, June 2). *CVE-2021-21974 Detail*. Retrieved from National Vulnerability Database: https://nvd.nist.gov/vuln/detail/CVE-2021-21974

SecurityWeek. (2023, February 6). *VMware ESXi Servers Targeted in Ransomware Attack via Old Vulnerability*. Retrieved from securityweek.com: https://www.securityweek.com/many-vmware-esxi-servers-targeted-in-ransomware-attack-via-old-vulnerability/

VMware. (2021, July 13). *Addressing VMSA-2021-0014*. Retrieved from VMware communities: https://communities.vmware.com/t5/vSphere-Upgrade-Install/Addressing-VMSA-2021-0014/ta-p/2857173

VMware. (2023, February 13). *How to Disable/Enable the SLP Service on VMware ESXi (76372)*. Retrieved from VMware knowledge base: https://kb.vmware.com/s/article/76372

VMware. (2023, February 6). *VMware Security Response Center (vSRC) Response to 'ESXiArgs' Ransomware Attacks*. Retrieved from VMware Security Blog: https://blogs.vmware.com/security/2023/02/83330.html