



CVE-2021-21987

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2021-21987
State	PUBLIC
Assigner	security@vmware.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-24 12:15:00 UTC
Updated	2021-06-04 19:32:00 UTC
Description	VMware Workstation (16.x prior to 16.1.2) and Horizon Client for Windows (5.x prior to 5.5.2) contain out-of-bounds read vul

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows	-	All	All	All
Application	Vmware	Horizon Client	All	All	All	All
Application	Vmware	Workstation	All	All	All	All

References

Reference	Source	Link	Tags
VMSA-2021-0009	MISC	www.vmware.com	
ZDI-21-608 Zero Day Initiative	MISC	www.zerodayinitiative.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[375600](#) VMware Workstation and Horizon Client for Windows Multiple Vulnerabilities (VMSA-2021-0009)

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)