



Netwrix Auditor Insecure Object Deserialization Vulnerability

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2022-31199
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-11-08 01:15:00 UTC
Updated	2022-11-09 19:33:00 UTC
Description	Remote code execution vulnerabilities exist in the Netwrix Auditor User Activity Video Recording component affecting both 1

Risk And Classification

EPSS: 0.058550000 probability, percentile 0.906450000 (date 2026-05-17)

CISA KEY: Listed on 2023-07-11; due 2023-08-01; ransomware use Known

Problem Types: CWE-502

CISA Known Exploited Vulnerability

Vendor	Netwrix
Product	Auditor
Name	Netwrix Auditor Insecure Object Deserialization Vulnerability
Required Action	Apply updates per vendor instructions or discontinue use of the product if updates are unavailable.
Notes	Patch application requires login to customer portal: https://security.netwrix.com/Account/SignIn?ReturnUrl=%2FAdvisories%2FADV-2022-003 ; https://nvd.nist.gov/vuln/detail/CVE-2022-31199

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netwrix	Auditor	All	All	All	All

References

Reference	Source	Link	Tags
Netwrix Auditor Application Critical Vulnerability... Bishop Fox	MISC	bishopfox.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev
No vendor comments have been submitted for this CVE.			
Legacy QID Mappings			
377863 Netwrix Auditor Remote Code Execution (RCE) Vulnerability			

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

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