Kentico Xperience <= 13.0.178 Staging Media File Upload Authenticated RCE

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-2749
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-03-24 19:15:52 UTC
Updated	2026-04-21 12:48:29 UTC
Description	An authenticated remote code execution in Kentico Xperience allows authenticated users Staging Sync Server to upload ar

Risk And Classification

Primary CVSS: v3.1 7.2 HIGH from disclosure@vulncheck.com

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.050510000 probability, percentile 0.897970000 (date 2026-04-29)

CISA KEV: Listed on 2026-04-20; due 2026-05-04; ransomware use Unknown

Problem Types: CWE-22 | CWE-434 | CWE-22 CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | CWE-434 CWE-434 Unrestricted Upload of File with Dangerous Type

Version	Source	Type	Score	Severity	Vector
3.1	disclosure@vulncheck.com	Secondary	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

CISA Known Exploited Vulnerability

Vendor	Kentico
Product	Kentico Xperience
Name	Kentico Xperience Path Traversal Vulnerability
Required Action	Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.
Notes	https://devnet.kentico.com/download/hotfixes ; https://nvd.nist.gov/vuln/detail/CVE-2025-2749

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kentico	Xperience	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Kentico	Xperience	affected 13.0.178 custom	Not specified

References

Reference	Source	Link
www.vulncheck.com/advisories/kentico-xperience-staging-media-file-upload-authen...	disclosure@vulncheck.com	www.vuln
labs.watchtowr.com/bypassing-authentication-like-its-the-90s-pre-auth-rce-chain-...	disclosure@vulncheck.com	labs.watc
devnet.kentico.com/download/hotfixes	disclosure@vulncheck.com	devnet.ke
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91b3-4a467353bcc0	www.cisa
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa

Vendor Comments And Credit

Discovery Credit

CNA: Piotr Bazydlo (watchTowr) (en)

Additional Advisory Data

Source	Time	Event
ADP	2026-04-20T00:00:00.000Z	CVE-2025-2749 added to CISA KEV

There are currently no legacy QID mappings associated with this CVE.

© 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 registred 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**