



CVE-2019-10068

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2019-10068
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-03-26 18:29:00 UTC
Updated	2020-04-15 16:15:00 UTC
Description	An issue was discovered in Kentico 12.0.x before 12.0.15, 11.0.x before 11.0.48, 10.0.x before 10.0.52, and 9.x versions. D

Risk And Classification

EPSS: 0.938080000 probability, percentile 0.998620000 (date 2026-04-29)

CISA KEV: Listed on 2022-03-25; due 2022-04-15; ransomware use Unknown

Problem Types: CWE-502

CISA Known Exploited Vulnerability

Vendor	Kentico
Product	Xperience
Name	Kentico Xperience Deserialization of Untrusted Data Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2019-10068

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
Kentico CMS 12.0.14 Remote Command Execution ~ Packet Storm	MISC	packetstormsecurity.com	
DevNet - Hotfixes	MISC	devnet.kentico.com	Product, Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical

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

[379489](#) Kentico Deserialization of Untrusted Data Vulnerability

[730179](#) Kentico CMS Simple Object Access Protocol (SOAP) Deserialization 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