

CVE-2019-10068

Kentico Xperience Deserialization of Untrusted Data Vulnerability

Exigent

CISA KEV since Mar 25, 2022

Actively exploited

Public exploit module (Metasploit)

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. Due to a failure to validate security headers, it was possible for a specially crafted request to the staging service to bypass the initial authentication and proceed to deserialize user-controlled .NET object input. This deserialization then led to unauthenticated remote code execution on the server where the Kentico instance was hosted.

EVRS 86/100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.951 99.87th percentile · FIRST	CISA DEADLINE Apr 15, 2022 KEV since 2022 · listed over a year
--	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.951 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
xperience	$\geq 9.0.0 \leq 9.0.51$ $\geq 10.0.0 < 10.0.52$ $\geq 11.0.0 < 11.0.48$ $\geq 12.0.0 < 12.0.15$	after 9.0.51 · 10.0.52 · 11.0.48 · 12.0.15	NVD

Sources

Vendor guidance github.com/advisories/GHSA-f7w4-79f7-fhp3

Additional guidance devnet.kentico.com/download/hotfixes#securityBugs-v12

NVD nvd.nist.gov/vuln/detail/CVE-2019-10068

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2019-2129

Current data evulnable.com/vulnerability-management/cve/CVE-2019-10068

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.