

## Components:

kentico kentico \*

## 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. 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.

## Main problems:

502 "Deserialization of Untrusted Data"