

Components:

laravel laravel *

Description:

In Laravel Framework through 5.5.40 and 5.6.x through 5.6.29, remote code execution might occur as a result of an unserialize call on a potentially untrusted X-XSRF-TOKEN value. This involves the decrypt method in Illuminate/Encryption/Encrypter.php and PendingBroadcast in gadgetchains/Laravel/RCE/3/chain.php in phpdbg. The attacker must know the application key, which normally would never occur, but could happen if the attacker previously had privileged access or successfully accomplished a previous attack.

Main problems:

502 "Deserialization of Untrusted Data"