Use of a Broken or Risky Cryptographic Algorithm

Low **RCheesley** published **GHSA-x7g2-wrrp-r6h3** on Aug 30, 2021

Package

mautic/core (PHP)

Affected versions	Patched versions
< 3.3.4, < 4.0.0-rc	3.3.4, 4.0.0

Description

✍️ Description

The function mt_rand is used to generate session tokens, this function is cryptographically flawed due to its nature being one pseudorandomness, an attacker can take advantage of the cryptographically insecure nature of this function to enumerate session tokens for accounts that are not under his/her control

🕵️ Proof of Concept

Numerous examples and attack implementations can be found in this paper . If you're looking for a practical tool that can crack your mt_rand implementation's seed value, see this project and run the following commands in a console with php5 and OpenWall's tool installed:

```
root$ php -r 'mt_srand(13333337); echo mt_rand( ), "\n";'
```

After that, copy the output (1863134308) and execute the following commands:

```
root$ gcc php_mt_seed.c -o php_mt_seedroot$ ./php_mt_seed 1863134308
```

After waiting ~1 minute you should have a few possible seeds corresponding to their PHP versions, next to your installed PHP version you should see something akin to:

seed = 0x00cb7359 = 13333337 (PHP 7.1.0+)
Hey, that's your seed!

💥 Impact

An attacker could takeover accounts at random by enumerating and using access tokens.

📝 References

- https://openwall.com/php_mt_seedhttps://crypto.di.uoa.gr/CRYPTO.SEC/Randomness_Attacks_files/paper.pdf
- mautic/app/bundles/PointBundle/Controller/TriggerController.php
  Line 187 in 5213e32
  ```
  187      $sessionId     = $pointTrigger['sessionId'] ?? 'mautic_'.sha1(uniqid(mt_rand(), true));
  ```
- https://github.com/mautic/mautic/releases/tag/3.3.4
- https://github.com/mautic/mautic/releases/tag/4.0.0

Severity

Low 3.5 / 10

CVSS base metrics	
Attack vector	Network
Attack complexity	Low
Privileges required	Low
User interaction	Required
Scope	Unchanged
Confidentiality	None
Integrity	None
Availability	Low

CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:L

CVE ID

CVE-2021-27913

Weaknesses

CWE-327

Credits

michaellrowley
mohit-rocks