MWR LABS

Security Advisory

OpenCart Predictable Password Reset Tokens

28/07/2017

Software	OpenCart
Affected Versions	v2.3.0.2 Confirmed Vulnerable
CVE Reference	TBD
Author	Dan Clifford
Severity	High
Vendor	https://www.opencart.com/

Description

OpenCart is an open source eCommerce platform that powers over 340,000 online stores.

Multiple vulnerabilities were discovered which when combined could provide an attacker with remote code execution against OpenCart installations.

Impact

An attacker that can register a user account or view basic CAPTCHAs generated by the application will be able to generate and predict the password reset tokens of any user account with a known email address, including those with administrator privileges.

A further issue within the administration panel could allow an attacker to gain remote code execution if the application utilises sendmail.

Cause

The application relies on PHP's mt_rand() as a source of entropy when generating password reset links and basic captcha images. The abuse of this functionality allows an attacker to predict password reset tokens.

Further to this, the application allows unfiltered user input to be used as the 5th parameter of PHP's mail() function which can lead to remote code execution when sendmail is being used as a mail transport agent.

Interim Workaround

Password reset functionality for the administrator's account can be disabled within the administration panel. The setting can be found under Settings >Server > Allow Forgotten Password.

As a temporary measure, to disable password reset functionality for user accounts, the following modification can be made to OpenCart's source code:

catalog/controller/account/reset.php:10

```
if (isset($this->request->get['code'])) {
        $code = $this->request->get['code']; //Original Code
        $code = ''; //Modified Code
} else {
        $code = '';
}
```

MWR has not verified the temporary workaround in-depth and therefore cannot attest to the robustness of this interim workaround. As the vendor has not been forthcoming with a patch to remediate the issue within an appropriate timescale, best attempts have been made to both highlight the weakness and allow management of the risk to organisations that would not be aware.

Solution

MWR advise applying the interim workaround listed above as the vendor has not yet made a patch available and no plan for addressing the issue has been communicated.

Technical Details

Full technical details will be released at a later date.

Detailed Timeline

Date	Summary
2017-01-24	Issue discovered
2017-01-30	Multiple attempts to contact OpenCart Support
2017-04-12	OpenCart Support acknowledge the report, notify MWR that the email has been forwarded to the appropriate parties
2017-05-04	MWR inform OpenCart of intention to publish issue details within two weeks

2017-05-09	MWR suggest patches for the project
2017-05-10	MWR provide access to a demo installation of OpenCart, proof of concept exploit and email accounts
2017-07-28	No patch forthcoming - public release of advisory