**Problem**

<https://github.com/domainmod/domainmod/issues/122>

reset.php handles “resetting”/changing an existing user’s password. The reset functionality uses PHP’s **time()** to derive the new password for the user that is attempting to change their password. This method of using time() to create a temporary password is **very deterministic** and allows an attacker to invoke the reset password functionality and reliably determine what the new password is, thus allowing for an account takeover.

**reset.php**

$new\_password = substr(md5(**time()**), 0, 8);

**Fix**

**reset.php**

new\_password = $user->**generatePassword(30);**

$new\_hash = $user->generateHash($new\_password);