Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG) in star7th/showdoc

0

✓ Valid Reported on Nov 18th 2021

Description

Logged in by LDAP will lead to a weak-password initialization，

```
 <?php
            ...
                if ($ldap_user == $username) {
                    //如果该用户不在数据库里，则帮助其注册
                    $userInfo = D("User")->isExist($username) ;
                    if(!$userInfo){
                        D("User")->register($ldap_user,$ldap_user.time());
                    }
                    $rs2=ldap_bind($ldap_conn, $dn , $password);// 【when th
                    if ($rs2) {//如果该用户不在数据库里，则帮助其注册
                       D("User")->updatePwd($userInfo['uid'], $password);
                       return $this->checkLogin($username,$password);
                    }
                }
            }
```

Proof of Concept

1) If there is a valid LDAP user , let's say named `tom` , once he activated his account(such as logged with a WRONG password: such `tom/123456`)
2) Then， a record will be add to the Database (by `D("User ")->register($ldap_user,$ldap_user.time());`), with a password like `tom1637248826` , but the change of password `D("User")->updatePwd($` won't work
3) Because we all know that the password is like `tom.time()` , and `time()` is one kind of pseudo-random number, we could easily use brute force tool (such as Burp Intruder) to got it.
4) Thus in this situation，an attacker could brute force the password of tom's, until getting the password of `tom1637248826`

```
 if ($rs2) {//如果该用户不在数据库里，则帮助其注册
                       D("User")->updatePwd($userInfo['uid'], $password);
                       return $this->checkLogin($username,$password);
                    }
```

Impact

This vulnerability is capable of： compromise a user by brute force his/her password in certain situation （log with a valid LDAP username but WRONG password）

References

- https://owasp.org/Top10/A02_2021-Cryptographic_Failures/
- https://cwe.mitre.org/data/definitions/338.html

CVE
CVE-2021-3990
(Published)

Vulnerability Type
CWE-338: Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)

Severity
Medium (6.5)

Visibility
Public

Status
Fixed

Found by

hi-unc1e

@hi-unc1e

unranked

Fixed by

star7th

@star7th

unranked

This report was seen 365 times.

We are processing your report and will contact the **star7th/showdoc** team within 24 hours. a year ago

We have contacted a member of the **star7th/showdoc** team and are waiting to hear back a year ago

star7th validated this vulnerability a year ago

hi-unc1e has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

star7th marked this as fixed in **2.9.13** with commit **a9886f** a year ago

star7th has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Jamie Slome a year ago Admin

CVE published! 🎉🎉

Sign in to join this conversation