**MEDIUM: Potentially Unsafe Code - mt\_rand**

Line: 74 - C:\Users\Jeremy\Downloads\lhc+web\_cli\_lib\_install.php

The application uses pseudo-random number generation that is not cryptographically secure. Carry out a manual check to ensure this is not being used in a process that requires cryptographically secure random numbers.

$cfgSite->setSetting( 'site', 'secrethash', substr(md5(time() . ":" . mt\_rand()),0,10));

**MEDIUM: Potentially Unsafe Code - md5**

Line: 74 - C:\Users\Jeremy\Downloads\lhc+web\_cli\_lib\_install.php

MD5 Hashing algorithm.

$cfgSite->setSetting( 'site', 'secrethash', substr(md5(time() . ":" . mt\_rand()),0,10));

**STANDARD: Potentially Unsafe Code - Use of Deterministic Pseudo-Random Values**

Line: 74 - C:\Users\Jeremy\Downloads\lhc+web\_cli\_lib\_install.php

The code appears to use the mt\_rand function. The resulting values, while appearing random to a casual observer, are predictable and may be enumerated by a skilled and determined attacker, although this is partly mitigated by a seed that does not appear to be time-based.

$cfgSite->setSetting( 'site', 'secrethash', substr(md5(time() . ":" . mt\_rand()),0,10));

**MEDIUM: Potentially Unsafe Code - mt\_rand**

Line: 124 - C:\Users\Jeremy\Downloads\lhc+web\_modules\_lhinstall\_install.php

The application uses pseudo-random number generation that is not cryptographically secure. Carry out a manual check to ensure this is not being used in a process that requires cryptographically secure random numbers.

$cfgSite->setSetting( 'site', 'secrethash', (!empty(getenv('LHC\_SECRET\_HASH')) ? getenv('LHC\_SECRET\_HASH') : substr(md5(time() . ":" . mt\_rand()),0,10)));

**MEDIUM: Potentially Unsafe Code - md5**

Line: 124 - C:\Users\Jeremy\Downloads\lhc+web\_modules\_lhinstall\_install.php

MD5 Hashing algorithm.

$cfgSite->setSetting( 'site', 'secrethash', (!empty(getenv('LHC\_SECRET\_HASH')) ? getenv('LHC\_SECRET\_HASH') : substr(md5(time() . ":" . mt\_rand()),0,10)));

**STANDARD: Potentially Unsafe Code - Use of Deterministic Pseudo-Random Values**

Line: 124 - C:\Users\Jeremy\Downloads\lhc+web\_modules\_lhinstall\_install.php

The code appears to use the mt\_rand function. The resulting values, while appearing random to a casual observer, are predictable and may be enumerated by a skilled and determined attacker, although this is partly mitigated by a seed that does not appear to be time-based.

$cfgSite->setSetting( 'site', 'secrethash', (!empty(getenv('LHC\_SECRET\_HASH')) ? getenv('LHC\_SECRET\_HASH') : substr(md5(time() . ":" . mt\_rand()),0,10)));