# CVE Detail – CVE-2016-10180

An issue was discovered on the D-Link DWR-932B router. WPS PIN generation is based on srand(time(0)) seeding.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.93083

## CVSS Scoring

CVSS v3.1 Score: 7.5

Severity: HIGH

## Mapped CWE(s)

* CWE-1241: Use of Predictable Algorithm in Random Number Generator
* CWE-330: Use of Insufficiently Random Values
* CWE-335: Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG)

## CAPEC(s)

* CAPEC-112: Brute Force
* CAPEC-485: Signature Spoofing by Key Recreation
* CAPEC-59: Session Credential Falsification through Prediction
* CAPEC-97: Cryptanalysis

## ATT&CK Techniques

* T1552.004: Private Keys
* T1110: Brute Force

## Used By (Actors/Tools)

* Machete (malware)
* Mafalda (malware)
* Hildegard (malware)
* Chaos (malware)
* FoggyWeb (malware)
* Caterpillar WebShell (malware)
* Pysa (malware)
* Troll Stealer (malware)
* Ebury (malware)
* Kinsing (malware)
* QakBot (malware)
* jRAT (malware)
* AADInternals (tool)
* Empire (tool)
* PoshC2 (tool)
* Mimikatz (tool)
* CrackMapExec (tool)
* Operation Wocao (campaign)
* Dragonfly (intrusion-set)
* OilRig (intrusion-set)
* Fox Kitten (intrusion-set)
* SolarWinds Compromise (campaign)
* Turla (intrusion-set)
* Ember Bear (intrusion-set)
* TeamTNT (intrusion-set)
* APT28 (intrusion-set)
* HEXANE (intrusion-set)
* Volt Typhoon (intrusion-set)
* 2016 Ukraine Electric Power Attack (campaign)
* APT39 (intrusion-set)
* APT38 (intrusion-set)
* Operation Dream Job (campaign)
* DarkVishnya (intrusion-set)
* APT41 (intrusion-set)
* Rocke (intrusion-set)
* Scattered Spider (intrusion-set)
* Agrius (intrusion-set)
* FIN5 (intrusion-set)

## Affected Products

* cpe:2.3:o:dlink:dwr-932b\_firmware:02.02eu:revb:\*:\*:\*:\*:\*:\*