# CVE Detail – CVE-2009-3278

The QNAP TS-239 Pro and TS-639 Pro with firmware 2.1.7 0613, 3.1.0 0627, and 3.1.1 0815 use the rand library function to generate a certain recovery key, which makes it easier for local users to determine this key via a brute-force attack.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.23048

## CVSS Scoring

CVSS v3.1 Score: 5.5

Severity: MEDIUM

## Mapped CWE(s)

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

## Affected Products

* cpe:2.3:o:qnap:ts-239\_pro\_firmware:2.1.7:build0613:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qnap:ts-239\_pro\_firmware:3.1.0:build0627:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qnap:ts-239\_pro\_firmware:3.1.1:build0815:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qnap:ts-639\_pro\_firmware:2.1.7:build0613:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qnap:ts-639\_pro\_firmware:3.1.0:build0627:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qnap:ts-639\_pro\_firmware:3.1.1:build0815:\*:\*:\*:\*:\*:\*