# CVE Detail – CVE-2018-12520

An issue was discovered in ntopng 3.4 before 3.4.180617. The PRNG involved in the generation of session IDs is not seeded at program startup. This results in deterministic session IDs being allocated for active user sessions. An attacker with foreknowledge of the operating system and standard library in use by the host running the service and the username of the user whose session they're targeting can abuse the deterministic random number generation in order to hijack the user's session, thus escalating their access.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.91483

## CVSS Scoring

CVSS v3.1 Score: 8.1

Severity: HIGH

## Mapped CWE(s)

* CWE-335: Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG)

## Affected Products

* cpe:2.3:a:ntop:ntopng:\*:\*:\*:\*:\*:\*:\*:\*