# CVE Detail – CVE-2008-2433

The web management console in Trend Micro OfficeScan 7.0 through 8.0, Worry-Free Business Security 5.0, and Client/Server/Messaging Suite 3.5 and 3.6 creates a random session token based only on the login time, which makes it easier for remote attackers to hijack sessions via brute-force attacks. NOTE: this can be leveraged for code execution through an unspecified "manipulation of the configuration."

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.93557

## CVSS Scoring

CVSS v3.1 Score: 9.8

Severity: CRITICAL

## Mapped CWE(s)

* CWE-330: Use of Insufficiently Random Values

## CAPEC(s)

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

## 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:a:trendmicro:client\_server\_messaging\_suite:3.5:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:trendmicro:client\_server\_messaging\_suite:3.6:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:trendmicro:officescan:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:trendmicro:worry-free\_business\_security:5.0:\*:\*:\*:\*:\*:\*:\*