# CVE Detail – CVE-2008-4122

Joomla! 1.5.8 does not set the secure flag for the session cookie in an https session, which makes it easier for remote attackers to capture this cookie by intercepting its transmission within an http session.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.03017

## CVSS Scoring

CVSS v3.1 Score: 7.5

Severity: HIGH

## Mapped CWE(s)

* CWE-319: Cleartext Transmission of Sensitive Information

## CAPEC(s)

* CAPEC-102: Session Sidejacking
* CAPEC-117: Interception
* CAPEC-383: Harvesting Information via API Event Monitoring
* CAPEC-477: Signature Spoofing by Mixing Signed and Unsigned Content
* CAPEC-65: Sniff Application Code

## ATT&CK Techniques

* T1040: Network Sniffing
* T1056.004: Credential API Hooking

## Used By (Actors/Tools)

* TrickBot (malware)
* cd00r (malware)
* JumbledPath (malware)
* RDFSNIFFER (malware)
* NOKKI (malware)
* VersaMem (malware)
* Ursnif (malware)
* Zeus Panda (malware)
* J-magic (malware)
* Emotet (malware)
* Regin (malware)
* Line Dancer (malware)
* FoggyWeb (malware)
* MESSAGETAP (malware)
* Zebrocy (malware)
* FinFisher (malware)
* Carberp (malware)
* ZxShell (malware)
* Penquin (malware)
* Impacket (tool)
* Empire (tool)
* PoshC2 (tool)
* Responder (tool)
* NBTscan (tool)
* Velvet Ant (intrusion-set)
* ArcaneDoor (campaign)
* Sandworm Team (intrusion-set)
* APT28 (intrusion-set)
* Kimsuky (intrusion-set)
* 2015 Ukraine Electric Power Attack (campaign)
* DarkVishnya (intrusion-set)
* PLATINUM (intrusion-set)
* Salt Typhoon (intrusion-set)
* APT33 (intrusion-set)

## Affected Products

* cpe:2.3:a:joomla:joomla\!:1.5.8:\*:\*:\*:\*:\*:\*:\*