# CVE Detail – CVE-2008-5784

V3 Chat - Profiles/Dating Script 3.0.2 allows remote attackers to bypass authentication and gain administrative access by setting the admin cookie to 1.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.86855

## CVSS Scoring

CVSS v3.1 Score: 9.8

Severity: CRITICAL

## Mapped CWE(s)

* CWE-565: Reliance on Cookies without Validation and Integrity Checking

## CAPEC(s)

* CAPEC-226: Session Credential Falsification through Manipulation
* CAPEC-31: Accessing/Intercepting/Modifying HTTP Cookies
* CAPEC-39: Manipulating Opaque Client-based Data Tokens

## ATT&CK Techniques

* T1539: Steal Web Session Cookie

## Used By (Actors/Tools)

* TRANSLATEXT (malware)
* Lumma Stealer (malware)
* DarkGate (malware)
* Chaes (malware)
* EVILNUM (malware)
* Spica (malware)
* BLUELIGHT (malware)
* Grandoreiro (malware)
* XLoader (malware)
* MgBot (malware)
* TajMahal (malware)
* Raccoon Stealer (malware)
* XCSSET (malware)
* QakBot (malware)
* CookieMiner (malware)
* LuminousMoth (intrusion-set)
* SolarWinds Compromise (campaign)
* APT42 (intrusion-set)
* Sandworm Team (intrusion-set)
* Kimsuky (intrusion-set)
* Scattered Spider (intrusion-set)
* Lotus Blossom (intrusion-set)
* Evilnum (intrusion-set)
* Star Blizzard (intrusion-set)

## Affected Products

* cpe:2.3:a:v3chat:v3\_chat\_profiles\_dating\_script:3.0.2:\*:\*:\*:\*:\*:\*:\*