# CVE Detail – CVE-2005-0408

CitrusDB 0.3.6 and earlier generates easily predictable MD5 hashes of the user name for the id\_hash cookie, which allows remote attackers to bypass authentication and gain privileges by calculating the MD5 checksum of the user name combined with the "boogaadeeboo" string, which is hard-coded in the $hidden\_hash variable.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.86348

## CVSS Scoring

CVSS v3.1 Score: 9.8

Severity: CRITICAL

## Mapped CWE(s)

* CWE-916: Use of Password Hash With Insufficient Computational Effort

## CAPEC(s)

* CAPEC-55: Rainbow Table Password Cracking

## ATT&CK Techniques

* T1110.002: Password Cracking

## Used By (Actors/Tools)

* Net Crawler (malware)
* Dragonfly (intrusion-set)
* FIN6 (intrusion-set)
* Night Dragon (campaign)
* Salt Typhoon (intrusion-set)
* APT3 (intrusion-set)

## Affected Products

* cpe:2.3:a:citrusdb:citrusdb:\*:\*:\*:\*:\*:\*:\*:\*