# CVE Detail – CVE-2021-41192

Redash is a package for data visualization and sharing. If an admin sets up Redash versions 10.0.0 and prior without explicitly specifying the `REDASH\_COOKIE\_SECRET` or `REDASH\_SECRET\_KEY` environment variables, a default value is used for both that is the same across all installations. In such cases, the instance is vulnerable to attackers being able to forge sessions using the known default value. This issue only affects installations where the `REDASH\_COOKIE\_SECRET or REDASH\_SECRET\_KEY` environment variables have not been explicitly set. This issue does not affect users of the official Redash cloud images, Redash's Digital Ocean marketplace droplets, or the scripts in the `getredash/setup` repository. These instances automatically generate unique secret keys during installation. One can verify whether one's instance is affected by checking the value of the `REDASH\_COOKIE\_SECRET` environment variable. If it is `c292a0a3aa32397cdb050e233733900f`, should follow the steps to secure the instance, outlined in the GitHub Security Advisory.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.99418

## CVSS Scoring

CVSS v3.1 Score: 8.1

Severity: HIGH

## Mapped CWE(s)

* CWE-1188: Initialization of a Resource with an Insecure Default

## CAPEC(s)

* CAPEC-665: Exploitation of Thunderbolt Protection Flaws

## ATT&CK Techniques

* T1542.002: Component Firmware
* T1556: Modify Authentication Process
* T1211: Exploitation for Defense Evasion

## Used By (Actors/Tools)

* Cyclops Blink (malware)
* Kessel (malware)
* Ebury (malware)
* SILENTTRINITY (tool)
* Velvet Ant (intrusion-set)
* ArcaneDoor (campaign)
* Equation (intrusion-set)
* APT28 (intrusion-set)
* FIN13 (intrusion-set)

## Affected Products

* cpe:2.3:a:redash:redash:\*:\*:\*:\*:\*:\*:\*:\*