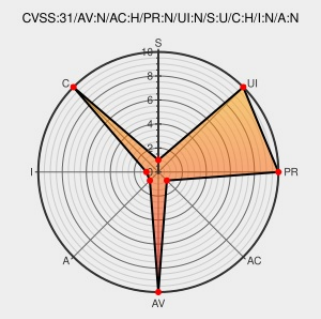
# CVE-2021-37588

Published on: 07/27/2021 12:00:00 AM UTC

Last Modified on: 08/09/2021 06:35:00 PM UTC

## CVE-2021-37588

Source: Mitre | Source: Nist | Print: PDF




Certain versions of Charm from Jhu contain the following vulnerability:

In Charm 0.43, any two users can collude to achieve the ability to decrypt YCT14 data.

CVE-2021-37588 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

### CVSS3 Score: 5.9 - MEDIUM

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---|---|---|---|
| NETWORK | HIGH | NONE | NONE |
| **Scope** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| UNCHANGED | HIGH | NONE | NONE |

### CVSS2 Score: 4.3 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | MEDIUM | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| PARTIAL | NONE | NONE |

### CVE References

| Description | Tags | Link |
|---|---|---|
| | www2.hci.uni-hannover.de<br>application/pdf | MISC www2.hci.uni-hannover.de/papers/Tan2019.pdf |
| No Description Provided | eprint.iacr.org<br>text/html | MISC eprint.iacr.org/2020/460 |

| | | |
|---|---|---|
| Broken schemes in last release · Issue #276 · JHUISI/charm · GitHub | github.com text/html | MISC github.com/JHUISI/charm/issues/276 |
| charm/abenc_yct14.py at dev · JHUISI/charm · GitHub | github.com text/html | MISC github.com/JHUISI/charm/blob/dev/charm/schemes/abenc/abenc_yct14.py |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Jhu | Charm | 0.43 | All | All | All |

cpe:2.3:a:jhu:charm:0.43:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

## Social Mentions

| Source | Title | Posted (UTC) |
|---|---|---|
| @CVEreport | CVE-2021-37588 : In Charm 0.43, any two users can collude to achieve the ability to decrypt YCT14 data.... cve.report/CVE-2021-37588 | 2021-07-27 23:42:36 |

← Previous ID

Next ID→