



# CVE-2021-37588

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

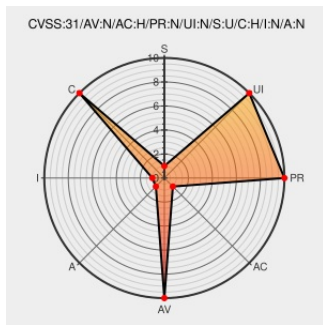
Last Modified on: 08/09/2021 06:35:00 PM UTC

## 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 [M](#) [cve@mitre.org](mailto: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
<b>NETWORK</b>	<b>HIGH</b>	<b>NONE</b>	<b>NONE</b>
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
<b>UNCHANGED</b>	<b>HIGH</b>	<b>NONE</b>	<b>NONE</b>

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
<b>NETWORK</b>	<b>MEDIUM</b>	<b>NONE</b>
Confidentiality Impact	Integrity Impact	Availability Impact
<b>PARTIAL</b>	<b>NONE</b>	<b>NONE</b>

## CVE References

Description	Tags	Link
	<a href="http://www2.hci.uni-hannover.de/application/pdf">www2.hci.uni-hannover.de application/pdf</a>	<a href="http://www2.hci.uni-hannover.de/papers/Tan2019.pdf">MISC www2.hci.uni-hannover.de/papers/Tan2019.pdf</a>
<b>No Description Provided</b>	<a href="http://eprint.iacr.org/text/html">eprint.iacr.org text/html</a>	<a href="http://eprint.iacr.org/2020/460">MISC eprint.iacr.org/2020/460</a>

Broken schemes in last release · Issue #276 · JHUISI/charm · GitHub

[github.com](#)  
[text/html](#)

MISC [github.com/JHUISI/charm/issues/276](https://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](https://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](mailto: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.... <a href="https://cve.report/CVE-2021-37588">cve.report/CVE-2021-37588</a>	2021-07-27 23:42:36

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2021 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)**