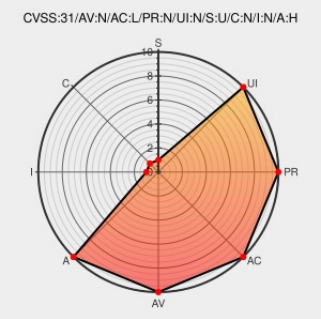
CVE-2021-40839

Published on: 09/09/2021 12:00:00 AM UTC

Last Modified on: 02/22/2022 02:48:00 PM UTC

CVE-2021-40839

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Fedora from Fedoraproject contain the following vulnerability:

The rencode package through 1.0.6 for Python allows an infinite loop in typecode decoding (such as via ;\x2f\x7f), enabling a remote attack that consumes CPU and memory.

CVE-2021-40839 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
[SECURITY] Fedora 34 Update: python-rencode-1.0.6-17.fc34 - package-announce - Fedora Mailing-Lists	Mailing List, Third Party Advisory, lists.fedoraproject.org, text/html	FEDORA FEDORA-2022-02340931ec

Full Disclosure: rencode 3-byte packet DoS	seclists.org text/html	MISC seclists.org/fulldisclosure/2021/Sep/16
Fix checking if typecode is valid while decoding. · aresch/rencode@572ff74 · GitHub	github.com text/html	MISC github.com/aresch/rencode/commit/572ff74586d9b1daab904c6f7f7009ce0143bb75
fix typecode decoding DoS by totaam · Pull Request #29 · aresch/rencode · GitHub	github.com text/html	MISC github.com/aresch/rencode/pull/29
[SECURITY] Fedora 35 Update: python-rencode-1.0.6-17.fc35 - package-announce - Fedora Mailing-Lists	Mailing List Third Party Advisory lists.fedoraproject.org text/html	FEDORA FEDORA-2022-1033a2718b
CVE-2021-40839 Python Vulnerability in NetApp Products | NetApp Product Security	security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20211008-0001/
rencode · PyPI	pypi.org text/html	MISC pypi.org/project/rencode/#history

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.

Related QID Numbers

183781 Debian Security Update for python-rencode (CVE-2021-40839)

282384 Fedora Security Update for python (FEDORA-2022-02340931ec)

282385 Fedora Security Update for python (FEDORA-2022-1033a2718b)

502924 Alpine Linux Security Update for py3-rencode

691120 Free Berkeley Software Distribution (FreeBSD) Security Update for py39 (70d0d2ec-cb62-11ed-956f-7054d21a9e2a)

980459 Python (pip) Security Update for rencode (GHSA-gh8j-2pgf-x458)

Exploit/POC from Github

Dirty Cow kernel exploit without libcrypt dependency

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Application	Rencode Project	Rencode	All	All	All	All

cpe:2.3:o:fedoraproject:fedora:34:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:35:*:*:*:*:*:*:*:

cpe:2.3:a:rencode_project:rencode:*:*:*:*:*:python:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-40839 : The rencode package through 1.0.6 for Python allows an infinite loop in typecode decoding such as… twitter.com/i/web/status/1…	2021-09-10 01:44:46
@0_exploit	CVE-2021-40839 dlvr.it/S7Jf0N	2021-09-10 12:32:04
@threatmeter	CVE-2021-40839 The rencode package through 1.0.6 for Python allows an infinite loop in typecode decoding (such as v… twitter.com/i/web/status/1…	2021-09-12 07:09:46

← Previous ID

Next ID→

© CVE.report 2023 |
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 registred 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