



CVE-2022-38766

Published on: Not Yet Published

Last Modified on: 01/10/2023 03:40:00 PM UTC

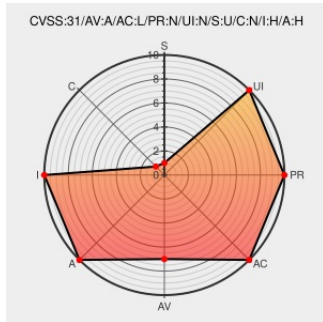
CVE-2022-38766

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of **Zoe E-tech** from **Renault** contain the following vulnerability:

The remote keyless system on Renault ZOE 2021 vehicles sends 433.92 MHz RF signals from the same Rolling Codes set for each door-open request, which allows for a replay attack.

CVE-2022-38766 has been assigned by [M cve@mitre.org](mailto:cve@mitre.org) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.1 - HIGH**

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

CVE References

Description	Tags	Link
GitHub - AUTOCRYPT-IVS-VnV/CVE-2022-38766: PoC for vulnerability in Renault ZOE Keyless System(CVE-2022-38766)	github.com text/html	MISC github.com/AUTOCRYPT-IVS-VnV/CVE-2022-38766

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

Exploit/POC from Github

[PoC for vulnerability in Renault ZOE Keyless System\(CVE-2022-38766\)](#)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Renault	Zoe E-tech	-	All	All	All
Operating System	Renault	Zoe E-tech Firmware	2021	All	All	All
<pre>cpe:2.3:h:renault:zoe_e-tech:-:*:*:*:*:*:*:</pre>						
<pre>cpe:2.3:o:renault:zoe_e-tech_firmware:2021:*:*:*:*:*:*:</pre>						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@ksg93rd	#exploit 1. CVE-2022-24637: Open web analytics info disclosure to RCE github.com/watchdog2000/c... 2. CVE-2022-38766: P... twitter.com/i/web/status/1...	2022-08-29 03:39:09
@hack_git	CVE-2022-38766 PoC for vulnerability in Renault ZOE Keyless System CVE-2022-38766 This vulnerability raised the q... twitter.com/i/web/status/1...	2022-08-29 07:10:56
@PentestingN	CVE-2022-38766 PoC for vulnerability in Renault ZOE Keyless System CVE-2022-38766 This vulnerability raised the q... twitter.com/i/web/status/1...	2022-08-29 10:14:13
@Securityblog	GitHub - AUTOCRYPT-IVS-VnV/CVE-2022-38766: PoC for vulnerability in Renault ZOE Keyless System(CVE-2022-38766) github.com/AUTOCRYPT-IVS-...	2022-09-06 06:59:14
@CVEreport	CVE-2022-38766 : The remote keyless system on Renault ZOE 2021 vehicles sends 433.92 MHz RF signals from the same R... twitter.com/i/web/status/1...	2023-01-03 15:05:39
/r/netcve	CVE-2022-38766	2023-01-03 15:38:41

[← Previous ID](#)

[Next ID →](#)

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](https://www.mitre.org/) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve/). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses/).

CVE.report and Source URL Uptime Status status.cve.report