

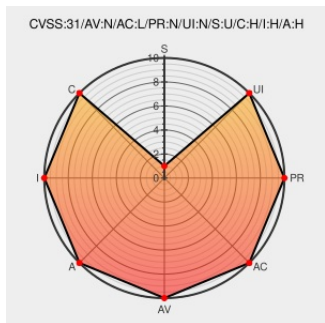


CVE-2022-2302

Published on: Not Yet Published

Last Modified on: 07/18/2022 02:18:00 PM UTC

CVE-2022-2302 - advisory for VDE-2022-030

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of **C520** from **Lenze** contain the following vulnerability:

Multiple Lenze products of the cabinet series skip the password verification upon second login. After a user has been logged on to the device once, a remote attacker can get full access without knowledge of the password.

CVE-2022-2302 has been assigned by [cert](#) info@cert.vde.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [cert](#) **LENZE** - cabinet c520 version < V01.08.01.3021

Affected Vendor/Software: [cert](#) **LENZE** - cabinet c550 version < V01.08.01.3021

Affected Vendor/Software: [cert](#) **LENZE** - cabinet c750 version < V01.08.01.3021

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **9.3 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link				
VDE-2022-030 CERT@VDE	cert.vde.com text/html	 CONFIRM cert.vde.com/en/advisories/VDE-2022-030/				
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
Hardware 	Lenze	C520	-	All	All	All
Operating System	Lenze	C520 Firmware	All	All	All	All
Hardware 	Lenze	C550	-	All	All	All
Operating System	Lenze	C550 Firmware	All	All	All	All
Hardware 	Lenze	C750	-	All	All	All
Operating System	Lenze	C750 Firmware	All	All	All	All
cpe:2.3:h:lenze:c520:-:*:*:*:*:*:						
cpe:2.3:o:lenze:c520_firmware:*:*:*:*:*:						
cpe:2.3:h:lenze:c550:-:*:*:*:*:*:						
cpe:2.3:o:lenze:c550_firmware:*:*:*:*:*:						
cpe:2.3:h:lenze:c750:-:*:*:*:*:*:						
cpe:2.3:o:lenze:c750_firmware:*:*:*:*:*:						
No vendor comments have been submitted for this CVE						
Social Mentions						
Source	Title					Posted (UTC)
 @CVEreport	CVE-2022-2302 : Multiple Lenze products of the cabinet series skip the password verification upon second login. Aft... twitter.com/i/web/status/1...					2022-07-11 10:46:48
 @vuldb	[Vuln] A severe vulnerability was disclosed for Lenze cabinet c520 and other products (CVE-2022-2302) vuldb.com/?id.203523					2022-07-11 12:26:39
 @Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-2302 Multiple Lenze products of the cabinet series skip the password ve... twitter.com/i/web/status/1...					2022-07-11 12:55:56
 /r/netsec	CVE-2022-2302					2022-07-11

[← 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 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](#)