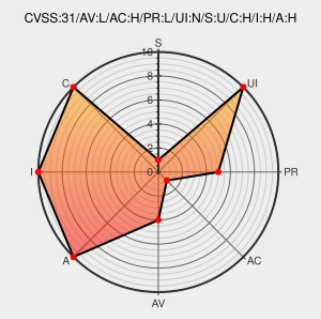
CVE-2022-29518

Published on: Not Yet Published

Last Modified on: 08/08/2023 02:21:00 PM UTC

CVE-2022-29518

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



Certain versions of Gc-a22w-cw from Koyoele contain the following vulnerability:

Screen Creator Advance2, HMI GC-A2 series, and Real time remote monitoring and control tool Screen Creator Advance2 versions prior to Ver.0.1.1.3 Build01, HMI GC-A2 series(GC-A22W-CW, GC-A24W-C(W), GC-A26W-C(W), GC-A24, GC-A24-M, GC-A25, GC-A26, and GC-A26-J2), and Real time remote monitoring and control tool(Remote GC) allows a local attacker to bypass authentication due to the improper check for the Remote control setting's account names. This may allow attacker who can access the HMI from Real time remote monitoring and control tool may perform arbitrary operations on the HMI. As a result, the information stored in the HMI may be disclosed, deleted or altered, and/or the equipment may be illegally operated via the HMI.

CVE-2022-29518 has been assigned by vultures@jpcert.or.jp to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **KOYO ELECTRONICS INDUSTRIES CO., LTD.** - **Screen Creator Advance2, HMI GC-A2 series, and Real time remote monitoring and control tool** version **Screen Creator Advance2 versions prior to Ver.0.1.1.3 Build01, HMI GC-A2 series(GC-A22W-CW, GC-A24W-C(W), GC-A26W-C(W), GC-A24, GC-A24-M, GC-A25, GC-A26, and GC-A26-J2), and Real time remote monitoring and control tool(Remote GC)**

CVSS3 Score: 7 - HIGH

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

CVSS2 Score: 5.9 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE

Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	COMPLETE

CVE References

Description	Tags	Link
[Update notice] Screen Creator Advance 2 software of GC-A2 Series | KOYO ELECTRONICS INDUSTRIES CO., LTD.	www.koyoele.co.jp text/html	MISC www.koyoele.co.jp/en/topics/202205095016/
JVN#50337155: KOYO Electronics Screen Creator Advance2 vulnerable to authentication bypass	jvn.jp text/xml	MISC jvn.jp/en/jp/JVN50337155/index.html

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	Koyoele	Gc-a22w-cw	-	All	All	All
Operating System	Koyoele	Gc-a22w-cw Firmware	-	All	All	All
Hardware	Koyoele	Gc-a24	-	All	All	All
Hardware	Koyoele	Gc-a24-m	-	All	All	All
Operating System	Koyoele	Gc-a24-m Firmware	-	All	All	All
Hardware	Koyoele	Gc-a24w-cw	-	All	All	All
Operating System	Koyoele	Gc-a24w-cw Firmware	-	All	All	All
Operating System	Koyoele	Gc-a24 Firmware	-	All	All	All
Hardware	Koyoele	Gc-a25	-	All	All	All
Operating System	Koyoele	Gc-a25 Firmware	-	All	All	All
Hardware	Koyoele	Gc-a26	-	All	All	All
Hardware	Koyoele	Gc-a26-j2	-	All	All	All
Operating System	Koyoele	Gc-a26-j2 Firmware	-	All	All	All
Hardware	Koyoele	Gc-a26w-cw	-	All	All	All
Operating System	Koyoele	Gc-a26w-cw Firmware	-	All	All	All

Operating System	Koyoele	Gc-a26 Firmware	-	All	All	All
Application	Koyoele	Remote Gc	-	All	All	All
Application	Koyoele	Screen Creator Advance 2	All	All	All	All
Application	Koyoele	Screen Creator Advance 2	0.1.1.3	-	All	All

cpe:2.3:h:koyoele:gc-a22w-cw:-:*:*:*:*:*:*:*:

cpe:2.3:o:koyoele:gc-a22w-cw_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:koyoele:gc-a24:-:*:*:*:*:*:*:*:

cpe:2.3:h:koyoele:gc-a24-m:-:*:*:*:*:*:*:*:

cpe:2.3:o:koyoele:gc-a24-m_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:koyoele:gc-a24w-c\(w\):-:*:*:*:*:*:*:*:

cpe:2.3:o:koyoele:gc-a24w-c\(w\)_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:o:koyoele:gc-a24_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:koyoele:gc-a25:-:*:*:*:*:*:*:*:

cpe:2.3:o:koyoele:gc-a25_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:koyoele:gc-a26:-:*:*:*:*:*:*:*:

cpe:2.3:h:koyoele:gc-a26-j2:-:*:*:*:*:*:*:*:

cpe:2.3:o:koyoele:gc-a26-j2_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:koyoele:gc-a26w-c\(w\):-:*:*:*:*:*:*:*:

cpe:2.3:o:koyoele:gc-a26w-c\(w\)_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:o:koyoele:gc-a26_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:a:koyoele:remote_gc:-:*:*:*:*:*:*:*:

cpe:2.3:a:koyoele:screen_creator_advance_2:*:*:*:*:*:*:*:*:

cpe:2.3:a:koyoele:screen_creator_advance_2:0.1.1.3:-:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-29518 : Screen Creator Advance2, HMI GC-A2 series, and Real time remote monitoring and control tool Screen… twitter.com/i/web/status/1…	2022-05-18 14:12:36
/r/netcve	CVE-2022-29518	2022-05-18

14:39:19

← 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