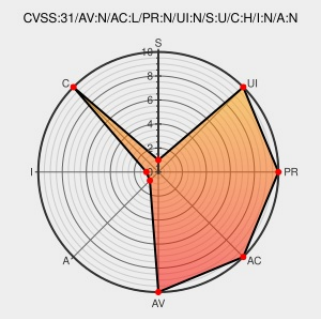
CVE-2021-3252

Published on: 02/23/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:52 PM UTC

CVE-2021-3252

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



Certain versions of Xp100u from Kaco-newenergy contain the following vulnerability:

KACO New Energy XP100U Up to XP-JAVA 2.0 is affected by incorrect access control. Credentials will always be returned in plain-text from the local server during the KACO XP100U authentication process, regardless of whatever passwords have been provided, which leads to an information disclosure vulnerability.

CVE-2021-3252 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	HIGH	NONE	NONE

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Kevin2600 auf Twitter: "https://t.co/aexDZzlChv… "	Third Party Advisory nitter.domain.glass text/html	MISC twitter.com/Kevin2600/status/1351189347501023238

Tiger-Team-1337: KACO XP100U HMI Credential Leak Vulnerability	Exploit Technical Description Third Party Advisory tiger-team-1337.blogspot.com text/html	MISC tiger-team-1337.blogspot.com/2021/01/kaco-xp100u-hmi-credential-leak.html
KACO HMI Hard-coded Password | CISA	Third Party Advisory US Government Resource us-cert.cisa.gov text/html	MISC us-cert.cisa.gov/ics/alerts/ICS-ALERT-15-224-01

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	Kaco-newenergy	Xp100u	-	All	All	All
Hardware	Kaco-newenergy	Xp100u	-	All	All	All
Hardware	Kaco-newenergy	Xp100u	-	All	All	All
Operating System	Kaco-newenergy	Xp100u Firmware	xp-java_2.0	All	All	All
Operating System	Kaco-newenergy	Xp100u Firmware	xp-java_2.0	All	All	All

cpe:2.3:h:kaco-newenergy:xp100u:-:*:*:*:*:*:*:*:

cpe:2.3:h:kaco-newenergy:xp100u:-:*:*:*:*:*:*:*:

cpe:2.3:h:kaco-newenergy:xp100u:-:*:*:*:*:*:*:*:

cpe:2.3:o:kaco-newenergy:xp100u_firmware:xp-java_2.0:*:*:*:*:*:*:*:

cpe:2.3:o:kaco-newenergy:xp100u_firmware:xp-java_2.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

site. This site includes MITRE data granted under the following license.

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