



CVE-2022-30997

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2022-30997
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-06-28 13:15:00 UTC
Updated	2022-07-08 03:15:00 UTC
Description	Use of hard-coded credentials vulnerability exists in STARDOM FCN Controller and FCJ Controller R4.10 to R4.31, which r

Risk And Classification

Problem Types: CWE-798

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Yokogawa	Stardom Fcj	-	All	All	All
Operating System	Yokogawa	Stardom Fcj Firmware	All	All	All	All
Hardware	Yokogawa	Stardom Fcn	-	All	All	All
Operating System	Yokogawa	Stardom Fcn Firmware	All	All	All	All

References

Reference	Source	Link	Tags
Yokogawa STARDOM CISA	MISC	www.cisa.gov	
web-material3.yokogawa.com/19/32885/files/YSAR-22-0007-J.pdf	MISC	web-material3.yokogawa.com	
web-material3.yokogawa.com/1/32885/files/YSAR-22-0007-E.pdf	MISC	web-material3.yokogawa.com	
JVNVU#95452299: YOKOGAWA STARDOMのコントローラーに複数の脆弱性	MISC	jvn.jp	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, and

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

© [CVE.report](#) 2026 |

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](#)