



CVE-2021-20827

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

Summary

CVE	CVE-2021-20827
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-24 07:15:00 UTC
Updated	2022-01-11 18:42:00 UTC
Description	Plaintext storage of a password vulnerability in IDEC PLCs (FC6A Series MICROSmart All-in-One CPU module v2.32 and e

Risk And Classification

Problem Types: CWE-312

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Idec	Data File Manager	All	All	All	All
Hardware	Idec	Microsmart Fc6a	-	All	All	All
Operating System	Idec	Microsmart Fc6a Firmware	All	All	All	All
Hardware	Idec	Microsmart Plus Fc6a	-	All	All	All
Operating System	Idec	Microsmart Plus Fc6a Firmware	All	All	All	All
Application	Idec	Windedit	All	All	All	All
Application	Idec	Windldr	All	All	All	All

References

Reference	Source	Link	Tags
JVNVU#92279973: Multiple vulnerabilities in IDEC PLCs	MISC	jvn.jp	
www.idec.com/home/lp/pdf/2021-12-24-PLC.pdf	MISC	www.idec.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)