CVE-2021-37400

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2021-37400
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-28 13:15:00 UTC
Updated	2022-01-07 20:40:00 UTC
Description	An attacker may obtain the user credentials from the communication between the PLC and the software. As a result, the PL

Risk And Classification

Problem Types: CWE-522

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	Ft1a Smartaxix Lite	-	All	All	All
Operating System	Idec	Ft1a Smartaxix Lite Firmware	All	All	All	All
Hardware	Idec	Ft1a Smartaxix Pro	-	All	All	All
Operating System	Idec	Ft1a Smartaxix Pro Firmware	All	All	All	All
Hardware	Idec	Microsmart Fc6a	-	All	All	All
Operating System	Idec	Microsmart Fc6a Firmware	All	All	All	All
Hardware	Idec	Microsmart Fc6b	-	All	All	All
Operating System	Idec	Microsmart Fc6b Firmware	All	All	All	All
Hardware	Idec	Microsmart Plus Fc6a	-	All	All	All
Operating System	Idec	Microsmart Plus Fc6a Firmware	All	All	All	All
Hardware	Idec	Microsmart Plus Fc6b	-	All	All	All
Operating System	Idec	Microsmart Plus Fc6b Firmware	All	All	All	All
Application	Idec	Windedit	All	All	All	All
Application	Idec	Windldr	All	All	All	All

References

Reference	Source	Link	Tags
FC6A MicroSmart | Micro PLC | Programmable Logic Controller | USA	MISC	us.idec.com	
www.idec.com/home/lp/pdf/2021-12-24-PLC.pdf	MISC	www.idec.com	
Automation Organizer | USA	MISC	us.idec.com	
JVNVU#92279973: Multiple vulnerabilities in IDEC PLCs	MISC	jvn.jp	
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.