CVE-2021-33843

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

Summary

CVE	CVE-2021-33843
State	PUBLIC
Assigner	ics-cert@hq.dhs.gov
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-01-21 19:15:00 UTC
Updated	2022-10-27 11:44:00 UTC
Description	Fresenius Kabi Agilia SP MC WiFi vD25 and prior has a default configuration page accessible without authentication. An at

Risk And Classification

Problem Types: CWE-306

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Fresenius-kabi	Agilia Connect	-	All	All	All
Operating System	Fresenius-kabi	Agilia Connect Firmware	All	All	All	All
Application	Fresenius-kabi	Agilia Partner Maintenance Software	All	All	All	All
Hardware	Fresenius-kabi	Agilia Sp Mc Wifi	-	All	All	All
Operating System	Fresenius-kabi	Agilia Sp Mc Wifi Firmware	All	All	All	All
Hardware	Fresenius-kabi	Link Agilia	-	All	All	All
Operating System	Fresenius-kabi	Link Agilia Firmware	All	All	All	All
Operating System	Fresenius-kabi	Link Agilia Firmware	3.0	-	All	All
Operating System	Fresenius-kabi	Link Agilia Firmware	3.0	d15	All	All
Application	Fresenius-kabi	Vigilant Centerium	1.0	All	All	All
Application	Fresenius-kabi	Vigilant Insight	1.0	All	All	All
Application	Fresenius-kabi	Vigilant Mastermed	1.0	All	All	All

References

Reference	Source	Link	Tags
Fresenius Kabi Agilia Connect Infusion System | CISA	MISC	www.cisa.gov	
CVE Program record	CVE.ORG	www.cve.org	canonical

NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

LEGACY: Julian Suleder (ERNW Research GmbH), Nils Emmerich (ERNW Research GmbH), Raphael Pavlidis (ERNW Research GmbH), and Dr. Oliver Matula (ERNW Enno Rey Netzwerke GmbH) reported these vulnerabilities to the German Federal Office for Information Security (BSI) in the context of the BSI project ManiMed (Medical Device Manipulation Project).

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