



# CVE-2021-41835

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

## Summary

|                        |                                                                                                                             |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2021-41835                                                                                                              |
| <b>State</b>           | PUBLIC                                                                                                                      |
| <b>Assigner</b>        | ics-cert@hq.dhs.gov                                                                                                         |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                |
| <b>Published</b>       | 2022-01-21 19:15:00 UTC                                                                                                     |
| <b>Updated</b>         | 2022-01-27 19:26:00 UTC                                                                                                     |
| <b>Description</b>     | Fresenius Kabi Agilia Link + version 3.0 does not enforce transport layer encryption. Therefore, transmitted data may be se |

## Risk And Classification

### Problem Types: CWE-319

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                         | Product                                             | Version | Update | Edition | Language |
|------------------|--------------------------------|-----------------------------------------------------|---------|--------|---------|----------|
| Hardware         | <a href="#">Fresenius-kabi</a> | <a href="#">Agilia Connect</a>                      | -       | All    | All     | All      |
| Operating System | <a href="#">Fresenius-kabi</a> | <a href="#">Agilia Connect</a>                      | All     | All    | All     | All      |
| Application      | <a href="#">Fresenius-kabi</a> | <a href="#">Agilia Partner Maintenance Software</a> | All     | All    | All     | All      |
| Hardware         | <a href="#">Fresenius-kabi</a> | <a href="#">Link Agilia</a>                         | -       | All    | All     | All      |
| Operating System | <a href="#">Fresenius-kabi</a> | <a href="#">Link Agilia Firmware</a>                | All     | All    | All     | All      |
| Operating System | <a href="#">Fresenius-kabi</a> | <a href="#">Link Agilia Firmware</a>                | 3.0     | -      | All     | All      |
| Operating System | <a href="#">Fresenius-kabi</a> | <a href="#">Link Agilia Firmware</a>                | 3.0     | d15    | All     | All      |
| Application      | <a href="#">Fresenius-kabi</a> | <a href="#">Vigilant Centerium</a>                  | 1.0     | All    | All     | All      |
| Application      | <a href="#">Fresenius-kabi</a> | <a href="#">Vigilant Insight</a>                    | 1.0     | All    | All     | All      |
| Application      | <a href="#">Fresenius-kabi</a> | <a href="#">Vigilant Mastermed</a>                  | 1.0     | All    | All     | All      |

## References

| Reference                                            | Source  | Link                                           | Tags                |
|------------------------------------------------------|---------|------------------------------------------------|---------------------|
| Fresenius Kabi Agilia Connect Infusion System   CISA | MISC    | <a href="http://www.cisa.gov">www.cisa.gov</a> |                     |
| CVE Program record                                   | CVE.ORG | <a href="http://www.cve.org">www.cve.org</a>   | canonical           |
| NVD vulnerability detail                             | NVD     | <a href="http://nvd.nist.gov">nvd.nist.gov</a> | 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.

© [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](#)