



# CVE-2023-47610

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

## Summary

|                        |                                                                                                                         |
|------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2023-47610                                                                                                          |
| <b>State</b>           | RESERVED                                                                                                                |
| <b>Assigner</b>        | cve@mitre.org                                                                                                           |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                            |
| <b>Published</b>       | 2023-11-09 17:15:00 UTC                                                                                                 |
| <b>Updated</b>         | 2023-11-16 17:19:00 UTC                                                                                                 |
| <b>Description</b>     | ** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new |

## Risk And Classification

### Problem Types: CWE-120

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                | Product                        | Version | Update | Edition | Language |
|------------------|-----------------------|--------------------------------|---------|--------|---------|----------|
| Hardware         | <a href="#">Telit</a> | <a href="#">Bgs5</a>           | -       | All    | All     | All      |
| Operating System | <a href="#">Telit</a> | <a href="#">Bgs5 Firmware</a>  | -       | All    | All     | All      |
| Hardware         | <a href="#">Telit</a> | <a href="#">Ehs5</a>           | -       | All    | All     | All      |
| Operating System | <a href="#">Telit</a> | <a href="#">Ehs5 Firmware</a>  | -       | All    | All     | All      |
| Hardware         | <a href="#">Telit</a> | <a href="#">Ehs6</a>           | -       | All    | All     | All      |
| Operating System | <a href="#">Telit</a> | <a href="#">Ehs6 Firmware</a>  | -       | All    | All     | All      |
| Hardware         | <a href="#">Telit</a> | <a href="#">Ehs8</a>           | -       | All    | All     | All      |
| Operating System | <a href="#">Telit</a> | <a href="#">Ehs8 Firmware</a>  | -       | All    | All     | All      |
| Hardware         | <a href="#">Telit</a> | <a href="#">Els61</a>          | -       | All    | All     | All      |
| Operating System | <a href="#">Telit</a> | <a href="#">Els61 Firmware</a> | -       | All    | All     | All      |
| Hardware         | <a href="#">Telit</a> | <a href="#">Els81</a>          | -       | All    | All     | All      |
| Operating System | <a href="#">Telit</a> | <a href="#">Els81 Firmware</a> | -       | All    | All     | All      |
| Hardware         | <a href="#">Telit</a> | <a href="#">Pds5</a>           | -       | All    | All     | All      |
| Operating System | <a href="#">Telit</a> | <a href="#">Pds5 Firmware</a>  | -       | All    | All     | All      |
| Hardware         | <a href="#">Telit</a> | <a href="#">Pds6</a>           | -       | All    | All     | All      |
| Operating System | <a href="#">Telit</a> | <a href="#">Pds6 Firmware</a>  | -       | All    | All     | All      |
| Hardware         | <a href="#">Telit</a> | <a href="#">Pds8</a>           | -       | All    | All     | All      |

|                  |                       |                                |   |     |     |     |
|------------------|-----------------------|--------------------------------|---|-----|-----|-----|
| Operating System | <a href="#">Telit</a> | <a href="#">Pds8 Firmware</a>  | - | All | All | All |
| Hardware         | <a href="#">Telit</a> | <a href="#">Pls62</a>          | - | All | All | All |
| Operating System | <a href="#">Telit</a> | <a href="#">Pls62 Firmware</a> | - | All | All | All |

References

| Reference                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------|
| KLCERT-23-018: Telit Cinterion (Thales/Gemalto) modules. Buffer Copy without Checking Size of Input vulnerability   Kaspersky ICS CERT |
| CVE Program record                                                                                                                     |
| NVD vulnerability detail                                                                                                               |

No vendor comments have been submitted for this CVE.

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