# CVE-2019-15809

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2019-15809 |
| **State** | PUBLIC |
| **Assigner** | cve@mitre.org |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2019-10-03 14:15:00 UTC |
| **Updated** | 2021-04-13 19:31:00 UTC |
| **Description** | Smart cards from the Athena SCS manufacturer, based on the Atmel Toolbox 00.03.11.05 and the AT90SC chip, contain a |

## Risk And Classification

**Problem Types:** CWE-203

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Athena-scs | Idprotect | 0106.0130.0401 | All | All | All |
| Operating System | Athena-scs | Idprotect | 010b.0352.0005 | All | All | All |
| Operating System | Athena-scs | Idprotect | 010e.1245.0002 | All | All | All |
| Operating System | Athena-scs | Idprotect | 0106.0130.0401 | All | All | All |
| Operating System | Athena-scs | Idprotect | 010b.0352.0005 | All | All | All |
| Operating System | Athena-scs | Idprotect | 010e.1245.0002 | All | All | All |
| Operating System | Cryptsoft | S/a Idflex V | 010b.0352.0005 | All | All | All |
| Operating System | Cryptsoft | S/a Idflex V | 010b.0352.0005 | All | All | All |
| Operating System | Cryptsoft | S/a Idflex V | 010b.0352.0005 | All | All | All |
| Application | Microchip | Atmel Toolbox | 00.03.11.05 | All | All | All |
| Application | Microchip | Toolbox | 00.03.11.05 | All | All | All |
| Application | Microchip | Toolbox | 00.03.11.05 | All | All | All |
| Operating System | Tecsec | Armored Card | 010e.0264.0001 | All | All | All |
| Operating System | Tecsec | Armored Card | 108.0264.0001 | All | All | All |
| Operating System | Tecsec | Armored Card | 010e.0264.0001 | All | All | All |
| Operating System | Tecsec | Armored Card | 108.0264.0001 | All | All | All |
| Operating System | Thalesgroup | Etoken 4300 | 010e.1245.0002 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Operating System | Thalesgroup | Etoken 4300 | 010e.1245.0002 | All | All | All |

## References

| Reference | Source | Link |
|---|---|---|
| Return of the Hidden Number Problem. \| IACR Transactions on Cryptographic Hardware and Embedded Systems | MISC | tches |
| minerva.crocs.fi.muni.cz | MISC | miner |
| eprint.iacr.org/2011/232.pdf | MISC | eprint |
| Bibliothèque cryptographique ATMEL Toolbox 00.03.11.05 \| Agence nationale de la sécurité des systèmes d'information | MISC | www. |
| Cryptographic Algorithm Validation Program \| CSRC | MISC | csrc.r |
| oss-security - Minerva: ECDSA key recovery from bit-length leakage | MLIST | www. |
| CVE Program record | CVE.ORG | www. |
| NVD vulnerability detail | NVD | nvd.n |

No vendor comments have been submitted for this CVE.

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