



# CVE-2019-15809

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2019-15809
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-10-03 14:15:00 UTC
<b>Updated</b>	2021-04-13 19:31:00 UTC
<b>Description</b>	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	<a href="#">Athena-scs</a>	<a href="#">Idprotect</a>	0106.0130.0401	All	All	All
Operating System	<a href="#">Athena-scs</a>	<a href="#">Idprotect</a>	010b.0352.0005	All	All	All
Operating System	<a href="#">Athena-scs</a>	<a href="#">Idprotect</a>	010e.1245.0002	All	All	All
Operating System	<a href="#">Athena-scs</a>	<a href="#">Idprotect</a>	0106.0130.0401	All	All	All
Operating System	<a href="#">Athena-scs</a>	<a href="#">Idprotect</a>	010b.0352.0005	All	All	All
Operating System	<a href="#">Athena-scs</a>	<a href="#">Idprotect</a>	010e.1245.0002	All	All	All
Operating System	<a href="#">Cryptsoft</a>	<a href="#">S/a Idflex V</a>	010b.0352.0005	All	All	All
Operating System	<a href="#">Cryptsoft</a>	<a href="#">S/a Idflex V</a>	010b.0352.0005	All	All	All
Operating System	<a href="#">Cryptsoft</a>	<a href="#">S/a Idflex V</a>	010b.0352.0005	All	All	All
Application	<a href="#">Microchip</a>	<a href="#">Atmel Toolbox</a>	00.03.11.05	All	All	All
Application	<a href="#">Microchip</a>	<a href="#">Toolbox</a>	00.03.11.05	All	All	All
Application	<a href="#">Microchip</a>	<a href="#">Toolbox</a>	00.03.11.05	All	All	All
Operating System	<a href="#">Tecsec</a>	<a href="#">Armored Card</a>	010e.0264.0001	All	All	All
Operating System	<a href="#">Tecsec</a>	<a href="#">Armored Card</a>	108.0264.0001	All	All	All
Operating System	<a href="#">Tecsec</a>	<a href="#">Armored Card</a>	010e.0264.0001	All	All	All
Operating System	<a href="#">Tecsec</a>	<a href="#">Armored Card</a>	108.0264.0001	All	All	All
Operating System	<a href="#">Thalesgroup</a>	<a href="#">Etoken 4300</a>	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	<a href="#">tches</a>
minerva.crocs.fi.muni.cz	MISC	<a href="#">miner</a>
eprint.iacr.org/2011/232.pdf	MISC	<a href="#">eprint</a>
Bibliothèque cryptographique ATMEL Toolbox 00.03.11.05   Agence nationale de la sécurité des systèmes d'information	MISC	<a href="#">www.</a>
Cryptographic Algorithm Validation Program   CSRC	MISC	<a href="#">csrc.r</a>
oss-security - Minerva: ECDSA key recovery from bit-length leakage	MLIST	<a href="#">www.</a>
CVE Program record	CVE.ORG	<a href="#">www.</a>
NVD vulnerability detail	NVD	<a href="#">nvd.n</a>

No vendor comments have been submitted for this CVE.

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](#)