



CVE-2008-2235

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

Summary

CVE	CVE-2008-2235
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-08-01 14:41:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	OpenSC before 0.11.5 uses weak permissions (ADMIN file control information of 00) for the 5015 directory on smart cards ;

Risk And Classification

Primary CVSS: v2.0 4.9 from nvd@nist.gov

AV:L/AC:L/Au:N/C:N/I:C/A:N

Problem Types: CWE-310 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

Complete

Availability

None

AV:L/AC:L/Au:N/C:N/I:C/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Opensc-project	Opensc	0.11.0	All	All	All

Application	Opensc-project	Opensc	0.11.1	All	All	All
Application	Opensc-project	Opensc	0.11.2	All	All	All
Application	Opensc-project	Opensc	0.11.3	All	All	All
Application	Opensc-project	Opensc	0.11.3	pre3	All	All
Application	Opensc-project	Opensc	0.11.4	All	All	All
Application	Opensc-project	Opensc	0.3.2	All	All	All
Application	Opensc-project	Opensc	0.3.5	All	All	All
Application	Opensc-project	Opensc	0.4.0	All	All	All
Application	Opensc-project	Opensc	0.6.0	All	All	All
Application	Opensc-project	Opensc	0.6.1	All	All	All
Application	Opensc-project	Opensc	0.7.0	All	All	All
Application	Opensc-project	Opensc	0.8	All	All	All
Application	Opensc-project	Opensc	0.8.0.0	All	All	All
Application	Opensc-project	Opensc	0.8.1	All	All	All
Application	Opensc-project	Opensc	0.9	All	All	All
Application	Opensc-project	Opensc	0.9.6	All	All	All
Application	Opensc-project	Opensc	0.9.7	All	All	All
Application	Opensc-project	Opensc	0.9.7	b	All	All
Application	Opensc-project	Opensc	0.9.7	d	All	All
Application	Opensc-project	Opensc	0.9.8	All	All	All
Operating System	Siemens	Cardos	m4	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

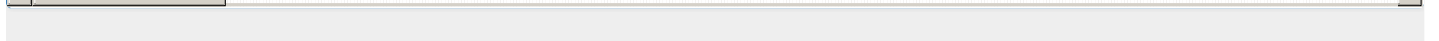
References						
Reference					Source	
OpenSC CardOS Improper Initialization Security Issue - Secunia Advisories - Vulnerability Information - Secunia.com					af854a3a-2127-422b-	
OpenSC Security Vulnerability and new Versions of OpenSC, OpenCT, LibP11, Pam_P11, Engine_PKCS11					af854a3a-2127-422b-	
[SECURITY] Fedora 9 Update: opensc-0.11.7-1.fc9					af854a3a-2127-422b-	
OpenSC: Insufficient protection of smart card PIN — Gentoo Linux Documentation					af854a3a-2127-422b-	
SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com					af854a3a-2127-422b-	
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:004					af854a3a-2127-422b-	
Fedora update for opensc - Secunia Advisories - Vulnerability Information - Secunia.com					af854a3a-2127-422b-	
Security Advisory SA33115 - Gentoo update for opensc - Secunia					af854a3a-2127-422b-	
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:010					af854a3a-2127-422b-	

[security-announce] SUSE Security Summary Report: SUSE-SA:2008:019	af854a3a-2127-422b-
Support / Security / Advisories // MDVSA-2008:183 Mandriva	af854a3a-2127-422b-
Debian update for opensc - Secunia Advisories - Vulnerability Intelligence - Secunia.com	af854a3a-2127-422b-
opensc-project.org Home of open source smart card solutions	af854a3a-2127-422b-
Debian -- Security Information -- DSA-1627-2 opensc	af854a3a-2127-422b-
OpenSC CardOS M4 Smart Cards Insecure Permissions Vulnerability	af854a3a-2127-422b-
IBM X-Force Exchange	af854a3a-2127-422b-
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD



Vendor Comments And Credit

Organization	Published	Contributor	Statement
Siemens	2008-08-14		Siemens has analyzed this report and states that no security breach can be found in the Siemens



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](#)