



CVE-2018-16421

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

Summary

CVE	CVE-2018-16421
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-09-04 00:29:00 UTC
Updated	2019-08-06 17:15:00 UTC
Description	Several buffer overflows when handling responses from a CAC Card in cac_get_serial_nr_from_CUID in libopensc/card-ca

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Opensc Project	Opensc	All	All	All	All

References

Reference	Source	Link	Tags
fixed out of bounds writes · OpenSC/OpenSC@360e95d · GitHub	MISC	github.com	Patch, Third Party Advis
Advisory X41-2018-002: Multiple Vulnerabilities in OpenSC X41 D-SEC GmbH	MISC	www.x41-dsec.de	Exploit, Third Party Advis
[SECURITY] [DLA 1916-1] opensc security update	MLIST	lists.debian.org	
Red Hat Customer Portal	REDHAT	access.redhat.com	
Release OpenSC-0.19.0-rc1 · OpenSC/OpenSC · GitHub	MISC	github.com	Patch, Release Notes, T
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[377236](#) Alibaba Cloud Linux Security Update for opensc (ALINUX2-SA-2019:0105)

[501105](#) Alpine Linux Security Update for opensc

© [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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)