

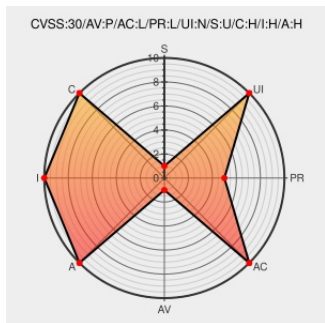


CVE-2018-16418

Published on: 09/03/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:33 PM UTC

CVE-2018-16418

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Opensc](#) from [Opensc Project](#) contain the following vulnerability:

A buffer overflow when handling string concatenation in util_acl_to_str in tools/util.c in OpenSC before 0.19.0-rc1 could be used by attackers able to supply crafted smartcards to cause a denial of service (application crash) or possibly have unspecified other impact.

CVE-2018-16418 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.6 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
PHYSICAL	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **4.6 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Advisory X41-2018-002: Multiple Vulnerabilities in OpenSC X41 D-SEC GmbH	Exploit Third Party Advisory www.x41-dsec.de text/html	X MISC www.x41-dsec.de/lab/advisories/x41-2018-002-OpenSC/

[SECURITY] [DLA 1916-1]
opensc security update

[lists.debian.org](#)
[text/html](#)

MLIST [debian-lts-announce] 20190911 [SECURITY] [DLA 1916-1] opensc security update

fixed out of bounds writes ·
OpenSC/OpenSC@360e95d
· GitHub

[Patch](#)
[Third Party Advisory](#)
[github.com](#)
[text/html](#)

MISC
github.com/OpenSC/OpenSC/commit/360e95d45ac4123255a4c796db96337f332160ad628c8445c4e7ae92bbc4be08ba11a4c3

Red Hat Customer Portal

[access.redhat.com](#)
[text/html](#)

 REDHAT RHSA-2019:2154

Release OpenSC-0.19.0-rc1
· OpenSC/OpenSC · GitHub

[Patch](#)
[Release Notes](#)
[Third Party Advisory](#)
[github.com](#)
[text/html](#)

MISC github.com/OpenSC/OpenSC/releases/tag/0.19.0-rc1

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

- 377236 Alibaba Cloud Linux Security Update for opensc (ALINUX2-SA-2019:0105)
- 501105 Alpine Linux Security Update for opensc

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Opensc Project	Opensc	All	All	All	All
cpe:2.3:a:opensc_project:opensc:*:*:*:*:*.*						

No vendor comments have been submitted for this CVE