

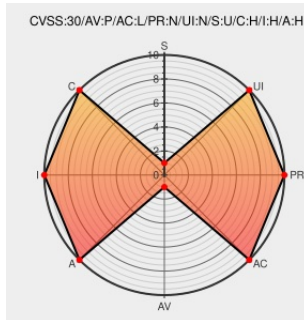


CVE-2018-16393

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

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

CVE-2018-16393

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

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

Several buffer overflows when handling responses from a Gemsafe V1 Smartcard in `gemsafe_get_cert_len` in `libopensc/pkcs15-gemsafeV1.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-2018-16393 has been assigned by [M](#) [cve@mitre.org](#) to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.8 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
PHYSICAL	LOW	NONE	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
fixed out of bounds writes · OpenSC/OpenSC@360e95d · GitHub	Patch Third Party Advisory github.com	MISC github.com/OpenSC/OpenSC/commit/360e95d45ac4123255a4c796db96337f332160ad

Advisory X41-2018-002: Multiple Vulnerabilities in OpenSC X41 D-SEC GmbH	text/html Exploit Third Party Advisory www.x41-dsec.de text/html	 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
Red Hat Customer Portal	access.redhat.com text/html	 REDHAT RHSA-2019:2154
Release OpenSC-0.19.0-rc1 · OpenSC/OpenSC · GitHub	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

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

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](#)