



CVE-2020-28975

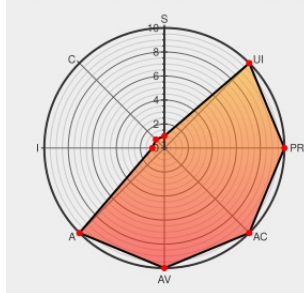
Published on: 11/21/2020 12:00:00 AM UTC

Last Modified on: 01/17/2023 06:24:00 PM UTC

CVE-2020-28975

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

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H



Certain versions of [Scikit-learn](#) from [Scikit-learn](#) contain the following vulnerability:

**** DISPUTED **** svm_predict_values in svm.cpp in Libsvm v324, as used in scikit-learn 0.23.2 and other products, allows attackers to cause a denial of service (segmentation fault) via a crafted model SVM (introduced via pickle, json, or any other model permanence standard) with a large value in the _n_support array. NOTE: the scikit-learn

vendor's position is that the behavior can only occur if the library's API is violated by an application that changes a private attribute.

CVE-2020-28975 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

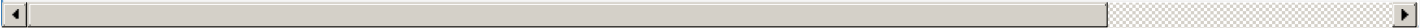
Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Scikit-Learn 0.23.2 Denial Of Service - PoC	CVE-2020-28975	https://msc.soaksternsecurity.com/files/160994/Scikit-Learn-0.23.2-Denial-Of-Service-PoC.pdf">https://msc.soaksternsecurity.com/files/160994/Scikit-Learn-0.23.2-Denial-Of-Service-PoC.pdf

Scikit-Learn 0.23.2 Denial Of Service ~ Packet Storm	Exploit Third Party Advisory packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/160261/Scikit-Learn-0.23.2-Denial-Of-Service/
Full Disclosure: scikit-learn 0.23.2 Local Denial of Service	Third Party Advisory seclists.org text/html	 FULLDISC 20201130 scikit-learn 0.23.2 Local Denial of Service
libsvm/svm.cpp at 9a3a9708926dec87d382c43b203f2ca19c2d56a0 · cjlin1/libsvm · GitHub	Exploit Third Party Advisory github.com text/html	 MISC github.com/cjlin1/libsvm/blob/9a3a9708926dec87d382c43b203f2ca19c2d56a0/libsvm/svm.cpp
FIX Prevents segfault in SVC when internals are altered (#21336) · scikit-learn/scikit-learn@1bf13d5 · GitHub	github.com text/html	 MISC github.com/scikit-learn/scikit-learn/commit/1bf13d567d3cd74854aa8343fd25b61dd768bb85
Segmentation fault on SVM LIB · Issue #18891 · scikit-learn/scikit-learn · GitHub	Exploit Third Party Advisory github.com text/html	 MISC github.com/scikit-learn/scikit-learn/issues/18891
scikit-learn: Denial of Service (GLSA 202301-03) — Gentoo security	security.gentoo.org text/html	 GENTOO GLSA-202301-03

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

[710704](#) Gentoo Linux scikit-learn Denial of Service (DoS) Vulnerability (GLSA 202301-03)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Scikit-learn	Scikit-learn	All	All	All	All
Application	Scikit-learn	Scikit-learn	0.23.2	All	All	All
Application	Scikit-learn	Scikit-learn	0.23.2	All	All	All
cpe:2.3:a:scikit-learn:scikit-learn:*:*:*:*:*:						
cpe:2.3:a:scikit-learn:scikit-learn:0.23.2:*:*:*:*:*:						
cpe:2.3:a:scikit-learn:scikit-learn:0.23.2:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)

© [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](#)