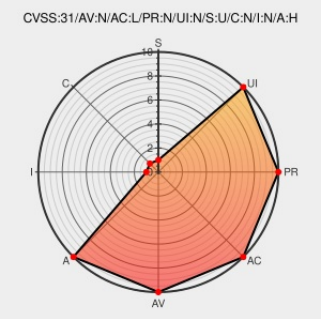
CVE-2020-28975

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



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 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 - Packet	Exploit	MISC packetstormsecurity.com/files/160281/SciKit-Learn-0.2

SciKit-Learn 0.23.2 Denial Of Service ≈ Packet Storm	Exploit Third Party Advisory packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/160281/SciKit-Learn-0.2
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 Serv
libsvm/svm.cpp at 9a3a9708926dec87d382c43b203f2ca19c2d56a0 · cjlin1/libsvm · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/cjlin1/libsvm/blob/9a3a9708926dec87d382c43b203f
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 SVMLIB · 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

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)

← Previous ID

Next ID→