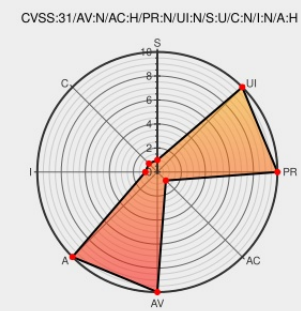
CVE-2022-42964

Published on: Not Yet Published

Last Modified on: 07/06/2023 01:52:00 PM UTC

CVE-2022-42964

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Pymatgen from Pymatgen contain the following vulnerability:

An exponential ReDoS (Regular Expression Denial of Service) can be triggered in the pymatgen PyPI package, when an attacker is able to supply arbitrary input to the GaussianInput.from_string method

CVE-2022-42964 has been assigned by security@jfrog.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **pymatgen** - **pymatgen** version **> 0**

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

CVE References

Description	Tags	Link
pymatgen ReDoS | XRAY-257184 - JFrog Security Research	research.jfrog.com text/html	MISC research.jfrog.com/vulnerabilities/pymatgen-redos-xray-257184/

Related QID Numbers

691130 Free Berkeley Software Distribution (FreeBSD) Security Update for py (951b513a-9f42-436d-888d-2162615d0fe4)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pymatgen	Pymatgen	-	All	All	All

cpe:2.3:a:pymatgen:pymatgen:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-42964 : An exponential ReDoS Regular Expression Denial of Service can be triggered in the pymatgen PyPI… twitter.com/i/web/status/1…	2022-11-09 19:59:39
/r/netcve	CVE-2022-42964	2022-11-09 20:38:11

← Previous ID

Next ID→