



# CVE-2021-27291

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2021-27291
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-03-17 13:15:00 UTC
<b>Updated</b>	2023-11-07 03:31:00 UTC
<b>Description</b>	In pygments 1.1+, fixed in 2.7.4, the lexers used to parse programming languages rely heavily on regular expressions. Som

## Risk And Classification

**Problem Types:** CWE-1333

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Application	<a href="#">Pygments</a>	<a href="#">Pygments</a>	All	All	All	All

## References

Reference	Source	Link
[SECURITY] [DLA 2648-1] mediawiki security update	MLIST	<a href="#">lists.debian</a>
Fix several exponential/cubic complexity regexes found by Ben Caller/... · pygments/pygments@2e7e8c4 · GitHub	MISC	<a href="#">github.com</a>
Debian -- Security Information -- DSA-4878-1 pygments	DEBIAN	<a href="#">www.debia</a>
[SECURITY] Fedora 33 Update: python-pygments-2.6.1-6.fc33 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedora</a>
[SECURITY] Fedora 32 Update: python-pygments-2.4.2-9.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedora</a>
cve-2021-27291 · GitHub	MISC	<a href="#">gist.github.com</a>
[SECURITY] [DLA 2648-2] mediawiki regression update	MLIST	<a href="#">lists.debian</a>
[SECURITY] Fedora 33 Update: python-pygments-2.6.1-6.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedora</a>
[SECURITY] Fedora 32 Update: python-pygments-2.4.2-9.fc32 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedora</a>

Debian -- Security Information -- DSA-4889-1 mediawiki	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>
[SECURITY] [DLA 2600-1] pygments security update	MLIST	<a href="http://lists.debian.org">lists.debian.org</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

- [159462](#) Oracle Enterprise Linux Security Update for python36:3.6 (ELSA-2021-4150)
- [159463](#) Oracle Enterprise Linux Security Update for python27:2.7 (ELSA-2021-4151)
- [159560](#) Oracle Enterprise Linux Security Update for resource-agents (ELSA-2021-9553)
- [178487](#) Debian Security Update for pygments (DLA 2600-1)
- [178489](#) Debian Security Update for pygments (DSA 4878-1)
- [178531](#) Debian Security Update for mediawiki (DSA 4889-1)
- [178584](#) Debian Security Update for mediawiki (DLA 2648-2)
- [178613](#) Debian Security Update for mediawiki (DLA 2648-1)
- [179545](#) Debian Security Update for mediawikipygments (CVE-2021-27291)
- [198315](#) Ubuntu Security Notification for Pygments Vulnerability (USN-4897-1)
- [199654](#) Ubuntu Security Notification for Pygments Vulnerabilities (USN-4897-2)
- [239582](#) Red Hat Update for python27 (RHSA-2021:3252)
- [239798](#) Red Hat Update for resource-agents security (RHSA-2021:4139)
- [239809](#) Red Hat Update for python36:3.6 (RHSA-2021:4150)
- [239826](#) Red Hat Update for python27:2.7 (RHSA-2021:4151)
- [281245](#) Fedora Security Update for python (FEDORA-2021-3f975f68c8)
- [281246](#) Fedora Security Update for python (FEDORA-2021-166dfc62b2)
- [296053](#) Oracle Solaris 11.4 Support Repository Update (SRU) 35.94.4 Missing (CPUJUL2021)
- [355592](#) Amazon Linux Security Advisory for python3-pygments : ALAS2-2023-2117
- [355791](#) Amazon Linux Security Advisory for python-pygments : ALAS2-2023-2198
- [501172](#) Alpine Linux Security Update for py3-pygments
- [670235](#) EulerOS Security Update for python-pygments (EulerOS-SA-2021-1841)

<a href="#">670337</a> EulerOS Security Update for python-pygments (EulerOS-SA-2021-1887)
<a href="#">670435</a> EulerOS Security Update for python-pygments (EulerOS-SA-2021-2065)
<a href="#">670446</a> EulerOS Security Update for python-pygments (EulerOS-SA-2021-2054)
<a href="#">670471</a> EulerOS Security Update for python-pygments (EulerOS-SA-2021-2228)
<a href="#">670683</a> EulerOS Security Update for python-pygments (EulerOS-SA-2021-2441)
<a href="#">751412</a> SUSE Enterprise Linux Security Update for python-Pygments (SUSE-SU-2021:3841-1)
<a href="#">751415</a> SUSE Enterprise Linux Security Update for python-Pygments (SUSE-SU-2021:3840-1)
<a href="#">751428</a> OpenSUSE Security Update for python-Pygments (openSUSE-SU-2021:3841-1)
<a href="#">751429</a> OpenSUSE Security Update for python-Pygments (openSUSE-SU-2021:3839-1)
<a href="#">751444</a> OpenSUSE Security Update for python-Pygments (openSUSE-SU-2021:1521-1)
<a href="#">900162</a> CBL-Mariner Linux Security Update for python-pygments 2.4.2
<a href="#">901938</a> Common Base Linux Mariner (CBL-Mariner) Security Update for python-pygments (6812-1)
<a href="#">903080</a> Common Base Linux Mariner (CBL-Mariner) Security Update for python-pygments (3982)
<a href="#">940186</a> AlmaLinux Security Update for resource-agents (ALSA-2021:4139)
<a href="#">940522</a> AlmaLinux Security Update for python27:2.7 (ALSA-2021:4151)
<a href="#">940566</a> AlmaLinux Security Update for python36:3.6 (ALSA-2021:4150)
<a href="#">960320</a> Rocky Linux Security Update for python27:2.7 (RLSA-2021:4151)
<a href="#">960392</a> Rocky Linux Security Update for python36:3.6 (RLSA-2021:4150)
<a href="#">960815</a> Rocky Linux Security Update for resource-agents (RLSA-2021:4139)
<a href="#">982634</a> Python (pip) Security Update for Pygments (GHSA-pq64-v7f5-gqh8)

© [CVE.report](#) 2026 |

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](#)