



CVE-2011-2765

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

Summary

CVE	CVE-2011-2765
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-08-20 13:29:00 UTC
Updated	2018-10-16 13:44:00 UTC
Description	pyro before 3.15 unsafely handles pid files in temporary directory locations and opening the pid file as root. An attacker can

Risk And Classification

Problem Types: CWE-59

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pyro Project	Pyro	All	All	All	All
Application	Pyro Project	Pyro	All	All	All	All

References

Reference	Source	Link	T
#631912 - pyro: pidfile in /tmp, opened insecurely [CVE-2011-2765] - Debian Bug report logs	CONFIRM	bugs.debian.org	E
PYRO - Change Log	CONFIRM	pythonhosted.org	V
changed pidfile location because of security vulnerability, debian bu... · irmen/Pyro3@554e095 · GitHub	CONFIRM	github.com	T
CVE Program record	CVE.ORG	www.cve.org	c:
NVD vulnerability detail	NVD	nvd.nist.gov	c:

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

980778 Python (pip) Security Update for pyro (GHSA-xrr4-74mc-rpjc)

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)