



CVE-2019-16784

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

Summary

CVE	CVE-2019-16784
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-14 20:15:00 UTC
Updated	2020-10-09 13:40:00 UTC
Description	In PyInstaller before version 3.6, only on Windows, a local privilege escalation vulnerability is present in this particular case

Risk And Classification

Problem Types: CWE-732

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Application	Pyinstaller	Pyinstaller	All	All	All	All
Application	Pyinstaller	Pyinstaller	All	All	All	All

References

Reference	Source
Local Privilege Escalation caused by insecure directory permissions of sys._MEIPATH · Advisory · pyinstaller/pyinstaller · GitHub	CONFIRM
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

LEGACY: This vulnerability was discovered and reported by Farid AYOUIJIL (@faridtsl), David HA, Florent LE NIGER and Yann GASCUEL (@Inv42) from Alter Solutions (@AlterSolutions) and fixed in collaboration with Hartmut Goebel (@htgoebel).

983071 Python (pip) Security Update for PyInstaller (GHSA-7fcj-pq9j-wh2r)

© [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](#)