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 AYOUJIL (@faridtsl), David HA, Florent LE NIGER and Yann GASCUEL (@Inv42) from Alter Solutions (@AlterSolutions) and fixed in collaboration with Hartmut Goebel (@htgoebel).

Legacy QID Mappings

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