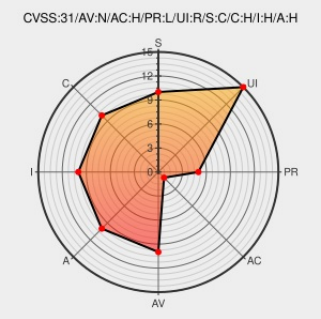
CVE-2022-21668

Published on: 01/10/2022 12:00:00 AM UTC

Last Modified on: 04/25/2022 05:58:00 PM UTC

CVE-2022-21668 - advisory for GHSA-qc9x-gjcv-465w

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



Certain versions of Fedora from Fedoraproject contain the following vulnerability:

pipenv is a Python development workflow tool. Starting with version 2018.10.9 and prior to version 2022.1.8, a flaw in pipenv's parsing of requirements files allows an attacker to insert a specially crafted string inside a comment anywhere within a requirements.txt file, which will cause victims who use pipenv to install the requirements file to download dependencies from a package index server controlled by the attacker. By embedding malicious code in packages served from their malicious index server, the attacker can trigger arbitrary remote code execution (RCE) on the victims' systems. If an attacker is able to hide a malicious `--index-url` option in a requirements file that a victim installs with pipenv, the attacker can embed arbitrary malicious code in packages served from their malicious index server that will be executed on the victim's host during installation (remote code execution/RCE). When pip installs from a source distribution, any code in the setup.py is executed by the install process. This issue is patched in version 2022.1.8. The GitHub Security Advisory contains more information about this vulnerability.

CVE-2022-21668 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **pypa** - **pipenv** version **>= 2018.10.9, < 2022.1.8**

CVSS3 Score: 8.6 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 9.3 - HIGH

Access Vector	Access Complexity	Authentication

NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Pipenv's requirements.txt parsing allows malicious index url in comments · Advisory · pypa/pipenv · GitHub	github.com text/html	CONFIRM github.com/pypa/pipenv/security/advisories/GHSA-qc9x-gjcv-465w
[SECURITY] Fedora 35 Update: pipenv-2021.5.29-7.fc35 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2022-77ce20f03a
Release Release v2022.1.8 · pypa/pipenv · GitHub	github.com text/html	MISC github.com/pypa/pipenv/releases/tag/v2022.1.8
Merge pull request from GHSA-qc9x-gjcv-465w · pypa/pipenv@439782a · GitHub	github.com text/html	MISC github.com/pypa/pipenv/commit/439782a8ae36c4762c88e43d5f0d8e563371b46f
[SECURITY] Fedora 36 Update: pipenv-2021.5.29-7.fc36 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2022-0d007466b3
[SECURITY] Fedora 34 Update: pipenv-2020.11.15-3.fc34 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2022-508e460384

Related QID Numbers

282471 Fedora Security Update for pipenv (FEDORA-2022-77ce20f03a)

282472 Fedora Security Update for pipenv (FEDORA-2022-508e460384)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All

Application	Pypa	Pipenv	All	All	All	All

cpe:2.3:o:fedoraproject:fedora:34:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:35:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:36:*:*:*:*:*:*:*:

cpe:2.3:a:pypa:pipenv:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-21668 : pipenv is a Python development workflow tool. Starting with version 2018.10.9 and prior to version… twitter.com/i/web/status/1…	2022-01-10 20:27:48
/r/netcve	CVE-2022-21668	2022-01-10 21:38:23

← Previous ID

Next ID→