

Vérification de la version Python ACI

Table des matières

[Introduction](#)

[Référence de version APIC Python](#)

[Prise en charge actuelle de Python](#)

[Exemple de vérification](#)

[Sécurité et compatibilité](#)

[Gestion des failles de sécurité](#)

[Évolutions futures](#)

[Références:](#)

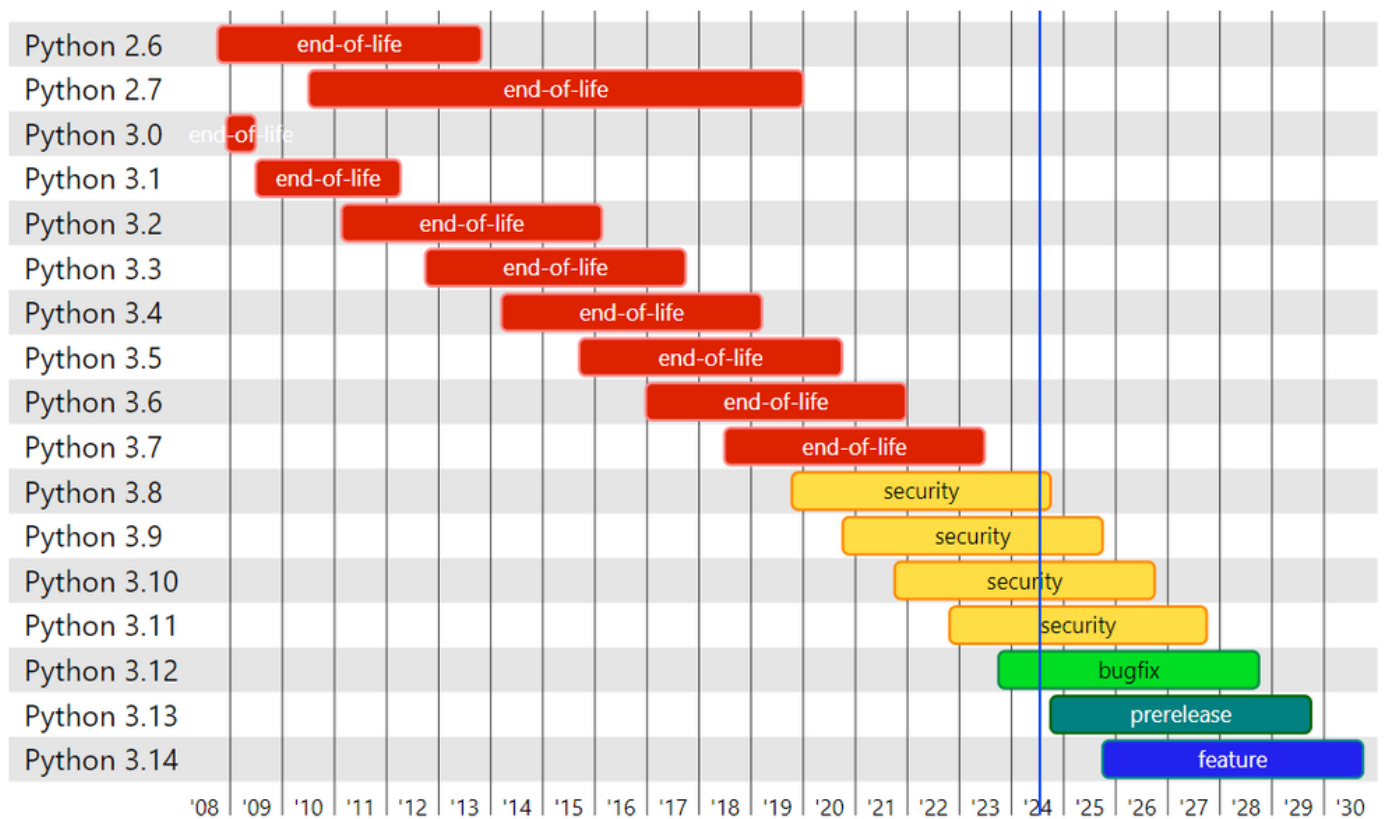
Introduction

Ce document décrit la politique de version de l'ACI Python et sa mise en oeuvre au sein de Cisco APIC.

Référence de version APIC Python

Cisco APIC prend en charge une gamme spécifique de versions Python rigoureusement testées et vérifiées pour garantir la compatibilité et la stabilité avec son logiciel. Les versions Python prises en charge peuvent varier selon la version du logiciel APIC.

Prise en charge actuelle de Python



Prise en charge actuelle de Python

Dans le cadre du Centre d'assistance technique (TAC), nous aidons souvent les clients à déterminer si une version différente de Python doit être installée pour résoudre une [vulnérabilité de sécurité](#). Un problème courant est la détection de Python Unsupported Version Detection, qui peut être marqué comme critique par divers scanners de sécurité.

Exemple :

Chemin : /

Port : 1733

Version installée : 3.7.6

Dernière version : 3.10

Dates d'assistance : 2023-06-27 (fin de vie)

Exemple de vérification

<#root>

APIC# acidiag version

6.0(5h)

```
APIC# python -V
```

```
Python 3.8.10
```

Les versions Python incluses dans les versions récentes du logiciel ACI sont les suivantes :

APIC version 5.2(8h) >= Python 2.7.17

APIC version 6.0(1) >= Python 3.7.6

APIC version 6.0(2) >= Python 3.8.10

Sécurité et compatibilité

Tous les scripts exécutés via le contrôleur APIC sont validés et testés par les développeurs Cisco. Ces scripts sont spécifiquement conçus pour la version Python incluse dans la version APIC respective.

La mise à jour vers une version Python différente, telle que 3.10, sur une version APIC initialement déployée avec une version antérieure peut modifier la façon dont les modules ACI interagissent. Cela peut entraîner des problèmes importants dans l'environnement. Les développeurs Cisco ne peuvent pas simplement réécrire les modules Python pour s'adapter à une nouvelle version, car la plupart des scripts DME (Data Management Engine) sont adaptés à des versions spécifiques de Python.

Gestion des failles de sécurité

Nos équipes de développement travaillent en permanence à identifier et à traiter les failles de sécurité sur tous les composants de l'ACI. Lorsqu'une vulnérabilité est découverte, elle est documentée sous un code CVE (Common Vulnerabilities and Exposures) et nos clients sont avertis rapidement de la prise de mesures appropriées. Cisco résout ces vulnérabilités par des mises à jour du microprogramme pour l'ACI, plutôt que par une mise à jour vers la dernière version de Python.

Évolutions futures

Des développements internes sont actuellement en cours pour intégrer Python 3.12 dans les prochaines versions d'APIC. Cela garantit que notre logiciel reste sécurisé et à jour avec les dernières avancées de Python tout en maintenant la compatibilité et la stabilité.

Références:

[Nessus - Détection de version non supportée de Python](#)

[État des versions de Python](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.