

ACI-Python-Version überprüfen

Inhalt

[Einleitung](#)

[APIC Python-Versionsreferenz](#)

[Unterstützung der aktuellen Python-Version](#)

[Verifizierungsbeispiel](#)

[Sicherheit und Kompatibilität](#)

[Management von Sicherheitslücken](#)

[Künftige Entwicklungen](#)

[Zugehörige Informationen](#)

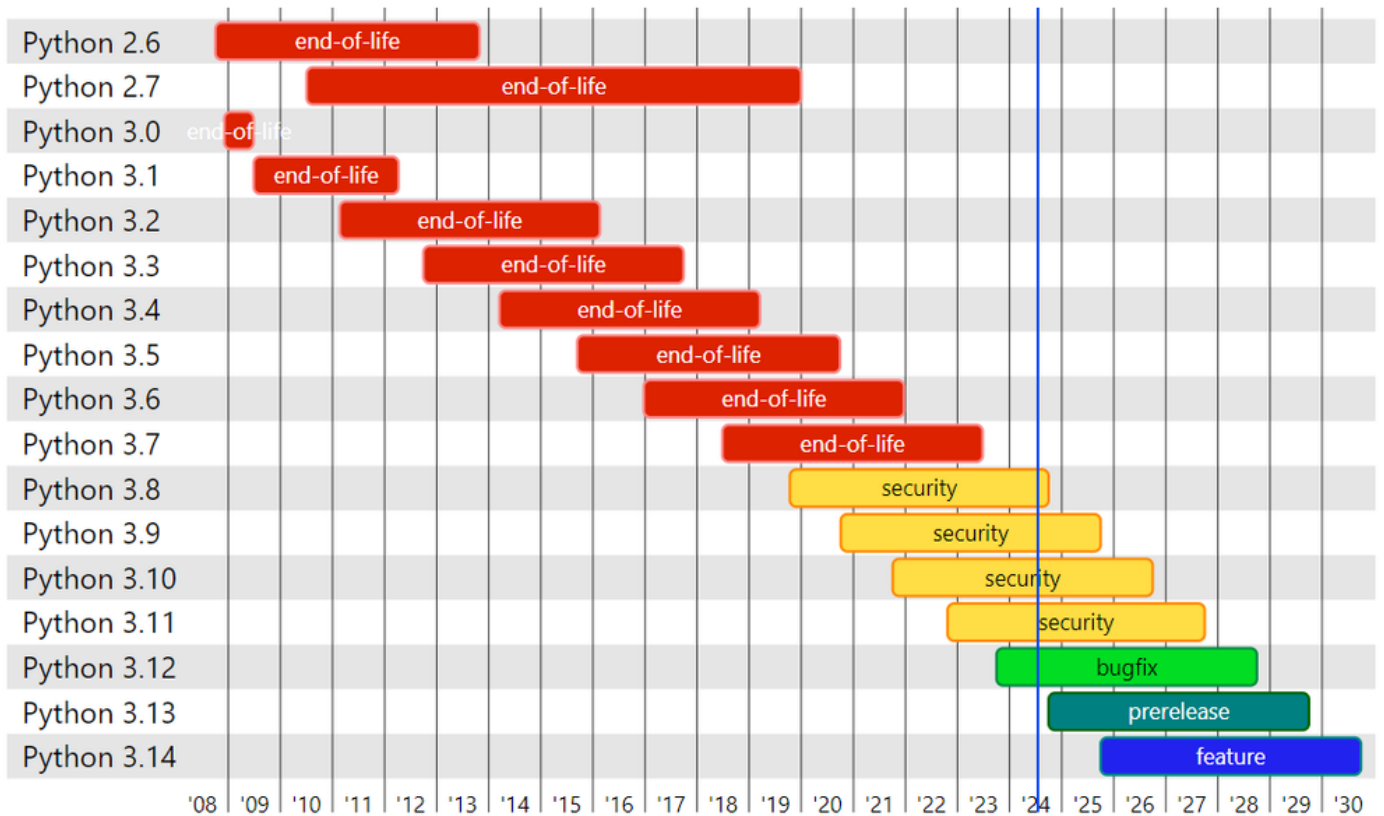
Einleitung

In diesem Dokument werden die ACI-Python-Versionsrichtlinie und ihre Implementierung im Cisco APIC beschrieben.

APIC Python-Versionsreferenz

Der Cisco APIC unterstützt eine Reihe von Python-Versionen, die rigorosen Tests unterzogen und überprüft wurden, um die Kompatibilität und Stabilität mit der Software sicherzustellen. Die unterstützten Python-Versionen können je nach APIC-Softwareversion variieren.

Unterstützung der aktuellen Python-Version



Unterstützung der aktuellen Python-Version

Das Technical Assistance Center (TAC) unterstützt Kunden bei der Entscheidung, ob eine andere Version von Python installiert werden muss, um [Sicherheitslücken](#) zu schließen. Ein häufiges Problem ist die Erkennung von Python Unsupported Version Detection, die von verschiedenen Sicherheitsscannern als kritisch markiert werden kann.

Beispiele:

Pfad: /

Hafen: 1733

Installierte Version: 3.7.6

Neueste Version: 3.10

Support-Termine: 2023-06-27 (end of life)

Verifizierungsbeispiel

<#root>

APIC# acidiag version

6.0(5h)

```
APIC# python -V
```

```
Python 3.8.10
```

Die Python-Versionen der neuesten ACI-Softwareversionen sind:

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

Sicherheit und Kompatibilität

Alle über den APIC ausgeführten Skripte werden von Cisco Entwicklern validiert und getestet. Diese Skripte wurden speziell für die Python-Version entwickelt, die in der jeweiligen APIC-Version enthalten ist.

Die Aktualisierung auf eine andere Python-Version (z. B. 3.10) einer APIC-Version, die ursprünglich mit einer früheren Version bereitgestellt wurde, kann die Interaktion der ACI-Module verändern. Dies kann zu erheblichen Problemen in der Umgebung führen. Cisco-Entwickler können die Python-Module nicht einfach umschreiben, um eine neue Version zu unterstützen, da die meisten DME-Skripts (Data Management Engine) auf bestimmte Python-Versionen zugeschnitten sind.

Management von Sicherheitslücken

Entwicklungsteams arbeiten kontinuierlich daran, Sicherheitslücken in allen ACI-Komponenten zu identifizieren und zu beseitigen. Wenn eine Schwachstelle entdeckt wird, wird sie unter einem CVE-Code (Common Vulnerabilities and Exposures) dokumentiert, und Kunden werden umgehend über geeignete Maßnahmen informiert. Cisco beseitigt diese Schwachstellen durch Firmware-Updates für die ACI, anstatt sie auf die neueste Python-Version zu aktualisieren.

Künftige Entwicklungen

Derzeit laufen interne Entwicklungen, um Python 3.12 in kommende APIC-Versionen zu integrieren. So wird sichergestellt, dass unsere Software mit den neuesten Python-Erweiterungen immer auf dem neuesten Stand ist und gleichzeitig die Kompatibilität und Stabilität gewährleistet bleibt.

Zugehörige Informationen

- [Nessus - Erkennung nicht unterstützter Python-Versionen](#)
- [Status der Python-Versionen](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.