

ACI Python 버전 확인

목차

[소개](#)

[APIC Python 버전 지정 참조](#)

[현재 Python 버전 지원](#)

[확인 예](#)

[보안 및 호환성](#)

[보안 취약성 관리](#)

[향후 개발](#)

[참조:](#)

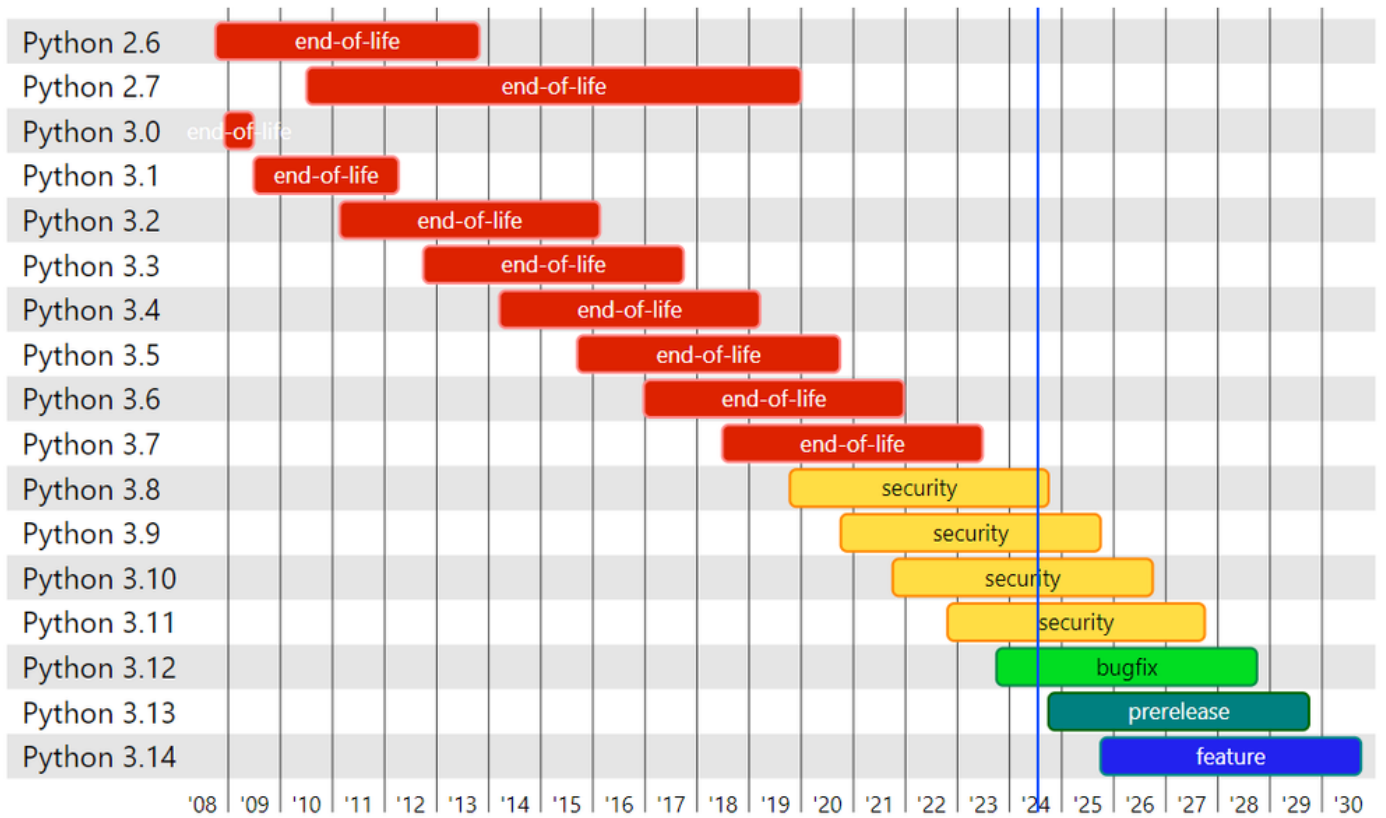
소개

이 문서에서는 ACI Python 버전 정책 및 Cisco APIC 내 구현에 대해 설명합니다.

APIC Python 버전 지정 참조

Cisco APIC는 소프트웨어와의 호환성 및 안정성을 보장하기 위해 엄격하게 테스트되고 검증된 특정 범위의 Python 버전을 지원합니다. 지원되는 Python 버전은 APIC 소프트웨어 릴리스에 따라 다를 수 있습니다.

현재 Python 버전 지원



현재 Python 버전 지원

TAC(Technical Assistance Center)의 일부로, [보안 취약성](#)을 해결하기 위해 다른 버전의 Python을 설치해야 하는지 여부를 확인하는 고객을 종종 [지원합니다](#). 한 가지 일반적인 문제는 Python Unsupported Version Detection의 탐지로, 다양한 보안 스캐너에서 Critical로 플래그를 지정할 수 있습니다.

예를 들면 다음과 같습니다.

경로: /

포트: 1733

설치된 버전: 3.7.6

최신 버전: 3.10

지원일: 2023-06-27(단종)

확인 예

<#root>

APIC# acidiag version

6.0(5h)

```
APIC# python -V
```

```
Python 3.8.10
```

최근 ACI 소프트웨어 릴리스에 포함된 Python 버전은 다음과 같습니다.

APIC 버전 5.2(8h) >= Python 2.7.17

APIC 버전 6.0(1) >= Python 3.7.6

APIC 버전 6.0(2) >= Python 3.8.10

보안 및 호환성

APIC를 통해 실행되는 모든 스크립트는 Cisco 개발자가 검증하고 테스트합니다. 이러한 스크립트는 해당 APIC 릴리스에 포함된 Python 버전을 위해 특별히 작성되었습니다.

원래 이전 버전과 함께 구축된 APIC 버전에서 3.10과 같은 다른 Python 버전으로 업데이트하면 ACI 모듈의 상호 작용 방식이 변경될 수 있습니다. 이로 인해 환경 내에서 중대한 문제가 발생할 수 있습니다. 대부분의 DME(Data Management Engine) 스크립트가 특정 Python 버전에 맞춰져 있기 때문에 Cisco 개발자는 새로운 버전을 수용하기 위해 Python 모듈을 재작성만 할 수는 없습니다.

보안 취약성 관리

Cisco 개발 팀은 모든 ACI 구성 요소에서 보안 침해를 식별하고 해결하기 위해 지속적으로 노력하고 있습니다. 취약성이 발견되면 CVE(Common Vulnerabilities and Exposures) 코드로 문서화되고 고객에게 적절한 조치를 취하도록 즉시 알립니다. Cisco는 최신 Python 버전으로 업데이트하는 대신 ACI용 펌웨어 업데이트를 통해 이러한 취약점을 해결합니다.

향후 개발

APIC의 향후 릴리스에 Python 3.12를 통합하기 위한 내부 개발이 현재 진행 중입니다. 이를 통해 Cisco 소프트웨어는 최신 Python의 향상된 기능을 통해 최신 상태로 안전하게 유지되면서 호환성과 안정성을 유지할 수 있습니다.

참조:

[Nessus - Python 지원되지 않는 버전 탐지](#)

[Python 버전 상태](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.