

Verificar la versión de ACI Python

Contenido

[Introducción](#)

[Referencia de versioning de APIC Python](#)

[Compatibilidad con la versión actual de Python](#)

[Ejemplo de verificación](#)

[Seguridad y compatibilidad](#)

[Gestión de vulnerabilidades de seguridad](#)

[Acontecimientos futuros](#)

[Referencias:](#)

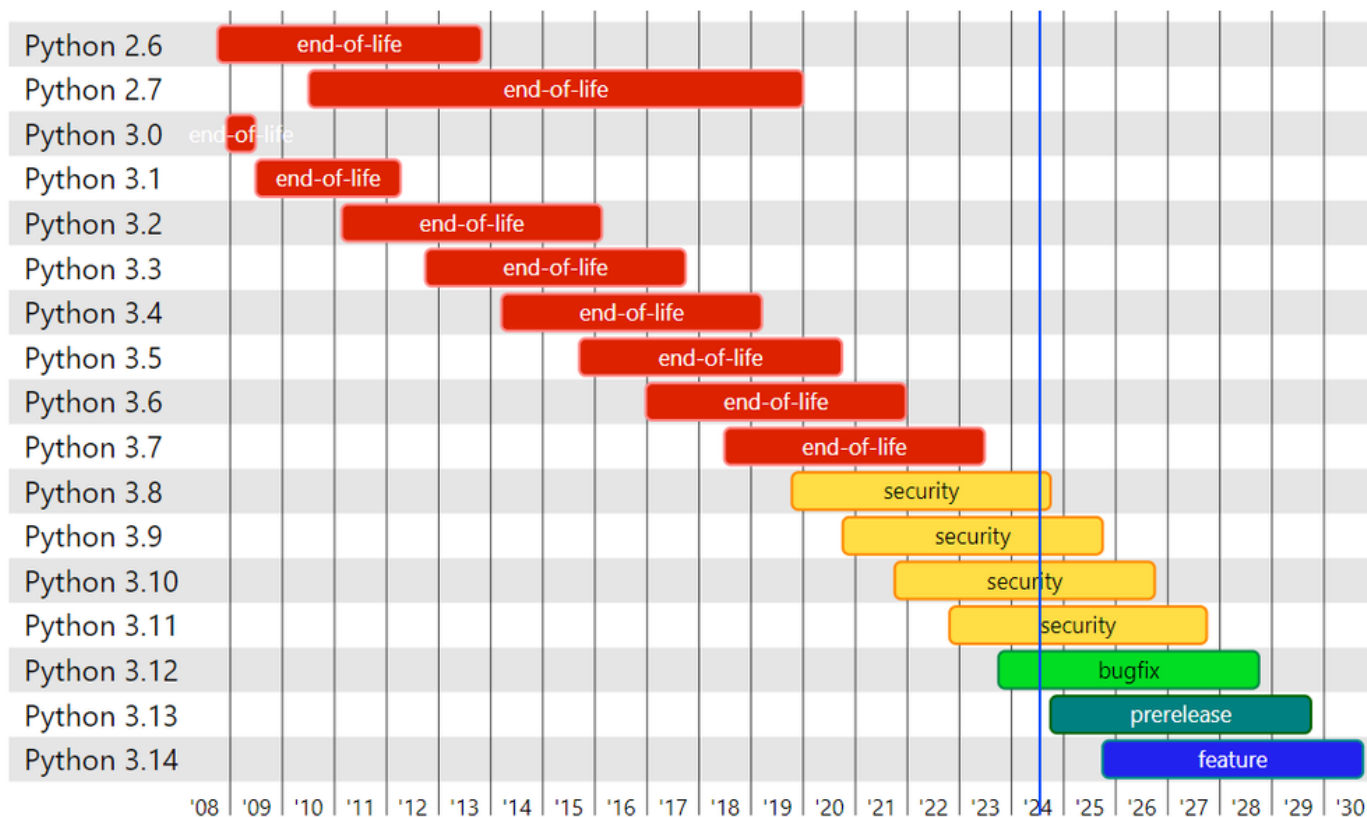
Introducción

Este documento describe la política de versión de ACI Python y su implementación dentro de Cisco APIC.

Referencia de versioning de APIC Python

Cisco APIC admite una serie específica de versiones de Python que se han probado y verificado rigurosamente para garantizar la compatibilidad y la estabilidad con su software. Las versiones compatibles de Python pueden variar en función de la versión de software de APIC.

Compatibilidad con la versión actual de Python



Compatibilidad con la versión actual de Python

Como parte del Technical Assistance Center (TAC), a menudo ayudamos a los clientes a determinar si es necesario instalar una versión diferente de Python para hacer frente a las [vulnerabilidades de seguridad](#). Un problema común es la detección de la detección de versiones no admitidas por Python, que varios escáneres de seguridad pueden señalar como críticas.

Por ejemplo:

Ruta : /

Puerto: 1733

Versión instalada: 3.7.6

Última versión: 3.10

Fechas de soporte: 2023-06-27 (fin de vida útil)

Ejemplo de verificación

<#root>

APIC# acidiag version

6.0(5h)

```
APIC# python -V
```

```
Python 3.8.10
```

Las versiones de Python incluidas en las últimas versiones de software de ACI son las siguientes:

APIC versión 5.2(8h) >= Python 2.7.17

APIC versión 6.0(1) >= Python 3.7.6

APIC versión 6.0(2) >= Python 3.8.10

Seguridad y compatibilidad

Todos los scripts ejecutados a través de APIC son validados y probados por los desarrolladores de Cisco. Estos scripts se crean específicamente para la versión de Python incluida en la versión de APIC correspondiente.

La actualización a una versión diferente de Python, como 3.10, en una versión APIC implementada originalmente con una versión anterior puede alterar la forma en que interactúan los módulos ACI. Esto podría causar problemas importantes en el entorno. Los desarrolladores de Cisco no pueden limitarse a reescribir los módulos de Python para adaptarlos a una nueva versión, ya que la mayoría de los scripts del motor de gestión de datos (DME) se adaptan a versiones específicas de Python.

Gestión de vulnerabilidades de seguridad

Nuestros equipos de desarrollo trabajan continuamente para identificar y abordar las brechas de seguridad en todos los componentes de ACI. Cuando se descubre una vulnerabilidad, se documenta mediante un código de exposiciones y vulnerabilidades habituales (CVE) y se notifica inmediatamente a nuestros clientes para que tomen las medidas adecuadas. Cisco aborda estas vulnerabilidades mediante actualizaciones de firmware para ACI, en lugar de actualizar a la versión más reciente de Python.

Acontecimientos futuros

Actualmente se están llevando a cabo desarrollos internos para integrar Python 3.12 en próximas versiones de APIC. Esto garantiza que nuestro software permanezca seguro y actualizado con los últimos avances de Python, a la vez que mantiene la compatibilidad y la estabilidad.

Referencias:

[Nessus - Detección de versiones no admitidas en Python](#)

[Estado de las versiones de Python](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).