Microsoft KB3161608/KB3161639를 설치한 후 CUIC 웹 페이지가 IE 11에서 로드되지 않음

목차

소개

이 문서에서는 Microsoft 기술 자료(KB) 업데이트 설치 후 Internet Explorer(IE)에서 Cisco CUIC(Unified Intelligence Center) 웹 페이지 로드를 중지하는 시나리오에 대해 설명합니다.

또한 CUIC의 관점에서 가능한 해결 방법/솔루션을 제공합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 주제에 대한 지식을 얻을 것을 권장합니다.

- Windows 관리
- CUIC 관리 및 구성

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

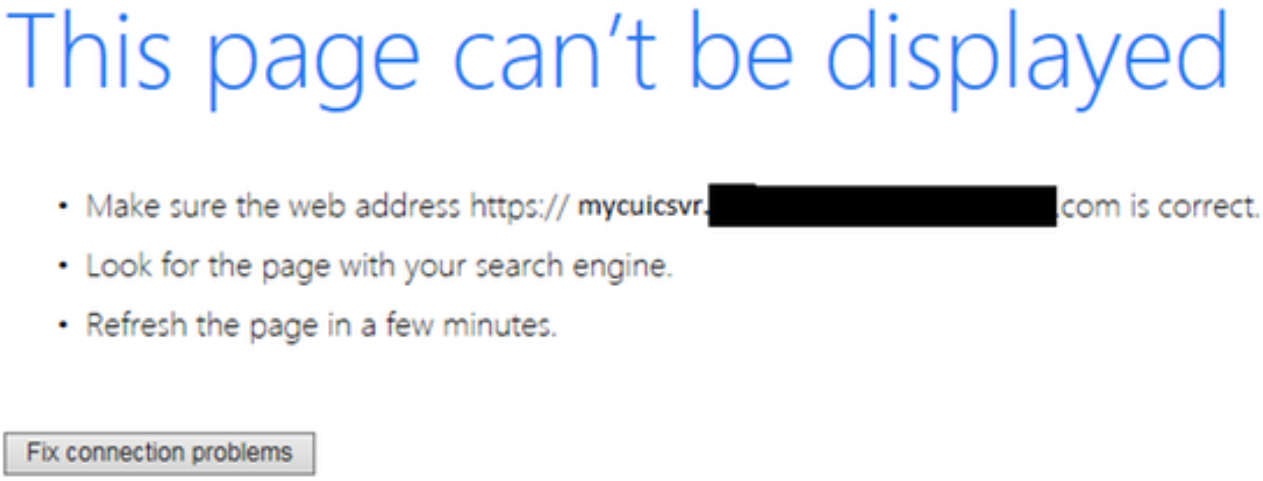
- Cisco Unified Intelligence Center 10.5(1)
- Cisco Unified Intelligence Center 10.x
- Cisco Unified Intelligence Center 9.1(x)
- Windows 7 또는 8
- Internet Explorer 11

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

시나리오

- CUIC 버전 9.1(1) 또는 CUIC 버전 10.5(1)
- Windows 7 또는 Windows 8의 IE(Internet Explorer) 11
- Windows 7/8에 KB3161639 설치
- Internet Explorer에서 CUIC 링크 시작 - http://<CUIC HOST ADDRESS>/*cuic*

이미지에 표시된 오류 메시지와 함께 메시지가 표시됩니다.



분석

Microsoft는 2016년 6월 업데이트 롤업 KB3161608의 일부로 새 암호 그룹을 추가했습니다.

Cipher suite	FIPS mode enabled	Protocols	Exchange	Encryption	Hash
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	Yes	TLS 1.2, TLS 1.1, TLS 1.0	DHE	AES	SHA1
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	Yes	TLS 1.2, TLS 1.1, TLS 1.0	DHE	AES	SHA1

KB3161639의 일부로서 **TLS_DHE_RSA_WITH_AES_128_CBC_SHA** 및 **TLS_DHE_RSA_WITH_AES_256_CBC_SHA**는 암호 그룹에 추가되고 Windows의 기본 순서는 변경됩니다. 운영 체제

따라서 클라이언트 시스템에 위의 업데이트가 있는 경우 CUIC tomcat 서버 (TLS_DHE_RSA_WITH_AES_**128_CBC_SHA**)와 CUIC tomcat 서버 (TLS_DHE_RSA_WITH_AES_128_CBC_SHA를 CUIC 구성 커넥터에 정의함)를 사용하여 통신하는 경향이 있습니다.

그러나 **TLS_DHE_RSA_WITH_AES_128_CBC_SHA** 암호를 사용하는 통신은 작동하지 않습니다 .이는 Microsoft에서 로그잼 공격을 해결하기 위해 적용하는 DHE(Diffie Hellman Exchange) 키에 대한 1024비트 최소 요구 사항 때문입니다.

11.x 버전까지의 CUIC에는 768비트 키만 지원하는 Java 6 버전이 있습니다.따라서 핸드셰이크 오류를 일으킬 수 있습니다.

솔루션

이 문제가 해결되는 CUIC 11.0(1)에는 적용되지 않습니다.CUIC 버전 9.1(1) 및 10.x 버전의 경우 여기에서 사용할 수 있는 개방형 SSL COP 파일에 의해 해결됩니다.

openssl cop의 일환으로 TLS_DHE_RSA_WITH_AES_128_CBC_SHA를 제거하여 CUIC tomcat 커넥터에서 DHE(Diffie-Hellman) 암호 지원이 제거됩니다.