문제: OpenSSL 취약점 CVE-2014-0160(하트블리드버그)

Software: ArcGIS Online Current **ArcGIS for Desktop** Advanced, Standard, Basic 10.1, 10.2, 10.2.1, 10.2.2 **ArcGIS for Server** 10.1, 10.2, 10.2.1, 10.2.2 **ArcGIS Runtime SDK for iOS** 10.2.2 **ArcGIS Runtime SDK for Android** 10.2.2 **ArcGIS Runtime SDK for Qt** 10.1.1, 10.2, 10.2.2**ArcGIS Runtime SDK for WPF** 10.1.1, 10.2, 10.2.2 **ArcGIS Runtime SDK for Java** 10.1.1, 10.2, 10.2.2 **ArcGIS Engine for Linux** 10.1, 10.2, 10.2.1, 10.2.2 **ArcGIS Engine for Windows** 10.1, 10.2, 10.2.1, 10.2.2 **ArcGIS Runtime SDK for OS X** 10.2.2
Platforms: N/A

개요

2014 년 4 월 7 일, OpenSSL 암호화 라이브러리를 실행하는 서버의 보안 취약점이 Heartbleed.com 에 의해 밝혀졌습니다. 이 보안 취약점에 대한 권고는 CVE-2014-0160 입니다. Esri 에서는 이 보안 취약점에 대해 Esri 고객을 보호하기 위해 Esri 서버와 인프라를 보안, 검증, 패치, 유지보수를 하고 있습니다.

많은 Esri 제품은 OpenSSL 를 포함하고 있지만, 그러나 이 것을 악용할 수 있는 방법으로는 사용할 수 없습니다. 보안 검색이 실제 보안 문제가 특정 사용에 존재하지 않는 경우에 CVE-2014-0160 을 기반으로 하는 라이브러리의 존재 플래그를 통해 시작할 것으로 예상됩니다. Esri 는 정상적으로 나타나는 거짓된 스캔을 제거하기 위해 제품의 OpenSSL 라이브러리를 업그레이드하는 소프트웨어 업데이트를 제공하고 있습니다.

원인

CVE-2014-0160 – OpenSSL 'Heartbleed' Vulnerability

방법

ArcGIS 제품과 서비스 사용자분 들은 필요한 작업을 확인하시려면 아래 요약을 확인하시기 바랍니다. 만약에 경우를 대비하여 마이그레이션이 완료될 때까지 패스워드 변경을 권장하고 있습니다.

1. 서비스
   A. ArcGIS Online – 모든 서비스와 인증서는 예방 조치로 플랫폼을 통해 실행되기 때문에 사용자들은 추가적인 작업이 필요하지 않습니다.
   B. 관리 서비스 – 인프라가 영향이 없기 때문에 사용자의 작업이 필요하지 않습니다.
   C. Esri 의 글로벌 계정 시스템 – 인프라에 영향이 없기 때문에 사용자의 작업이 필요하지 않습니다.

2. 데스크탑 제품
   A. ArcGIS for Desktop / Engine – 사용자의 작업이 필요하지 않습니다. OpenSSL 라이브러리가 ArcGIS Desktop 10.1 SP1, 10.2, 10.2.1, 10.2.2 에 포함되어 출시되었지만 이 취약점을 악용할 수 없습니다.
3. 서버 제품
   A. ArcGIS for Server (Windows) – 사용자의 조치가 필요하지 않습니다. 취약한 OpenSSL 라이브러리는 ArcGIS for Server 10.1 SP1, 10.2, 10.2.1, 10.2.2 에 포함하고 있지만 이를 악용할 수 있는 방법은 없습니다.
   B. ArcGIS for Server (Linux) – **Linux 에서 ArcGIS Server 10.2, 10.2.1, 10.2. 의 출력, 발행 서비스만 취약합니다.** Esri 는 이러한 문제를 해결하기 위해 보안패치 작업을 하고 Linux 에서는 이 서비스들을 필요에 따라 사용하지 못할 수 있습니다. 이에 대한 자세한 정보는 KB 42407 에서 찾을 수 있습니다.
   C. Portal for ArcGIS – 특별한 조치가 필요하지 않습니다.
   D. 웹 게이트웨이 – Esri 구성요소에는 포함하고 있지 않지만 사용자가 자신의 웹 서비스 앞 단에 OpenSSL 을 이용한 SSL 연결을 하고 있다면 공급 업체의 권장 사항에 따라 확인이 필요합니다. (예– 리버스 프록시, NAT)
4. Runtimes SDKs
   A. ArcGIS Runtime – 사용자의 조치가 필요하지 않습니다. Runtime WPF/Qt/Java 10.1.1, 10.2, 10.2.2 는 취약헌 OpenSSL 라이브러리가 포함되어 있지만 취약점을 악용할 수 있게 하지 않고 있습니다.

이에 Esri 에서는 OpenSSL 취약점을 개선하기 위한 패치를 제공하고 있습니다. 이 패치는 ArcGIS 10.2, 10.2.1, 10.2.2 for Server on Linux 를 사용하는 고객이라면 반드시 설치를 권장하고 있습니다.

ArcGIS 10.2 - 10.2.2 for Server OpenSSL (Heartbleed) Patch

http://support.esri.com/en/downloads/patches-servicepacks/view/productid/66/metaid/2088

관련 Esri 기술문서

Problem: OpenSSL Vulnerability CVE-2014-0160 (Heartbleed)

http://support.esri.com/en/knowledgebase/techarticles/detail/42405?WT.mc_id=EmailCampaigna35001

작성일: 2014/04/17

최종 수정일: 2014/04/25