장애보고서, 공지문
번역의 즐거움

– 기술문서 번역 모임 –

발표자는 이런 사람입니다

- 김현도 / 아카마이 코리아 재직
- (현) 기술영업팀 / (구) 기술지원팀
- 프로 삽질러 / 프로 사과러

적게 볼수록 좋은 것

- 장애 보고서
- 장애 공지문
- …

[redacted]에 관한

장애 보고서

[redacted]

장애 내역

대상 시간

[redacted]

장애 원인 및 대응

[redacted]

영향받은 서비스

[redacted]

사용자 영향도 분석

[redacted]

[redacted] CONFIDENTIAL

[redacted]

RCA for [redacted] – Not for Redistribution.

Root Cause Analysis

Executive Summary:

[redacted]

Problem Statement:

[redacted]

Time Chronology of Events [UTC]:

Date	Time	Action
[redacted]		

SWEET32 취약점에 관한 권고 사항 및 안내

Blog Post created by **Hyundo Kim** on Aug 25, 2016

Like • 0 Comment • 0

Akamai에서 SWEET32 취약점에 관한 권고 사항 및 안내를 드립니다.

최근에 알려진 DES-CBC3와 같은 cipher에 대한 공격은 보안성을 약화시켜 128bit 수준의 cipher를 유지하지 못하게 되어 RC4와 같은 수준의 위험성을 가지게 합니다.
이 공격은 BEAST attack와 비슷하며 브라우져 상에서의 악성 Javascript에 의해서만 노출될 수 있습니다.
Akamai는 DES-CBC3를 자사 서버측의 설정에서 삭제를 완료했으며 고객사에도 이와 동일한 처리를 할 것을 권고 드리는 바입니다.

현재 시점부터 Secure CDN에 새롭게 추가되는 secure용도의 도메인들은 **ak-akamai-default-2016q3**라는 cipher profile을 적용받게 되며 PCI DSS compliance가 필요한 고객들을 위해 DES-CBC3-SHA가 제외된 **ak-pci-dss-3.2** cipher profile가 준비되어 있으니 참고 부탁드립니다.

기존 secure용도의 도메인들을 사용하고 계신 고객사들은 위에 언급된 2개의 cipher profile중 하나로 TLS설정을 변경하도록 권고 드리는 바이며, 이는 보안에 취약한 DES-CBC3-SHA를 비활성화할 수 있는 방법중 하나입니다.

TLS cipher 설정을 변경하기 위해서는 Luna Control Center에 로그인 하여 "Configure"메뉴 하단의 SSL Certificate Management를 선택하시고 필요한 인증서를 선택하여 "Edit TLS Metadata"를 선택하시면 됩니다.
그 이후 ak-akamai-default-2016q3를 required, preferred cipher로 선택하시고 저장하시면 되며

SSL/TLS Cipher Profiles for Akamai Secure CDN

Nov 8, 2018 · Community Blog

Description

Web properties on Akamai's Secure CDN can be configured with various SSL/TLS cipher suites. Through our Certificate Provisioning System, customers can select a cipher profiles which, in turn, selects a list of cipher suites to be presented to connecting clients. Enumeration of the currently supported cipher profiles is below. Akamai does not update existing cipher profiles once enabled, except in the case of security incidents. **Not all ciphers listed in the profiles below are active on the Akamai Secure CDN.**

If a client presents the ChaCha20-Poly1305 cipher at the top of its preferred list, Akamai will move it to the top of the server-presented list, regardless of what is described below. This feature is to enable the best performance for those mobile devices which do not include AES acceleration hardware.

For PFS (Forward Secrecy) support, HTTP/2 support, and/or PCI and FedRAMP compliance, we recommend selecting the **ak-akamai-default-2017q3** or **ak-akamai-2018q3** cipher profile. All cipher suites in these profiles are suitable for PCI and FedRAMP traffic. The **ak-akamai-2018q3** profile can be used to avoid "weak cipher" warnings in SSL/TLS scanners at the expense of dropping support for older user agents which do not support Forward Secrecy ciphers. Secure properties that need to support connections from Internet Explorer on Windows XP or Windows Server 2000 must use the **ak-akamai-default-2016q1** profile or a custom cipher list which includes DES-CBC3-SHA.

If you have more specific needs around selecting individual cipher suites, please reach out to your account team or Customer Care.

Recommended Cipher Profiles

These profiles are available in Certificate Provisioning System and are recommended for use. Ciphers are listed below in the order they will be presented to clients.

번역의 두가지 의미

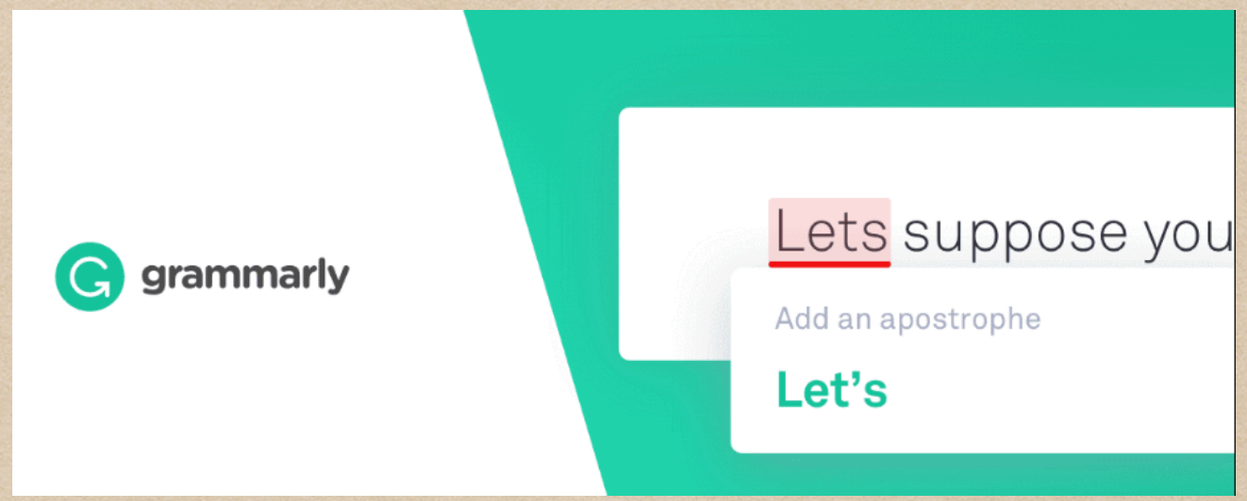
- 언어적 번역
- 상황적 번역

언어는 어렵습니다

- 영어:
  관사와 시제, 단수/복수 정도는 기본으로 틀립니다.
- 한글:
  상황에 맞는 적당한 표현과 문장력이 관건입니다

그래서 사용한 도구

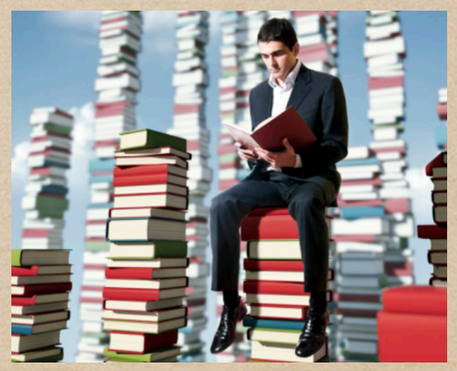
- 영어:



- 한글:

그런데 왜 즐겁습니까

- 간접 지식의 체득
- 뿌듯함



취미 번역

- Facebook Engineering Blog
  https://code.facebook.com