راه‌اندازی و پیکربندی امن پروتکل SSL/TLS بر روی سرویس‌دهنده پست الکترونیک Exim

شماره مستند APA-AMIRKABIR-13950705-1
تاریخ نگارش ..... ۵ مهر ۱۳۹۵
شماره نگارش ۱/۰
نگارش ..... آپای امیرکبیر
طبقه‌بندی ..... عادی

فهرست مطالب

۱ مقدمه

برای تأمین محرمانگی و جامعیت داده‌های مبادله شده می‌توان از پروتکل‌های استانداردی که بدین منظور طراحی شده استفاده کرد. در حال حاضر مهم‌ترین پروتکل رمزنگاری که در سطح اینترنت برای رمزنگاری داده‌های لایه کاربرد و تأمین امنیت ارتباطات استفاده می‌شود، پروتکل SSL/TLS است. در این گزارش مراحل نصب گواهی‌نامه SSL و امن‌سازی پروتکل SSL/TLS را بر روی سرویس‌دهنده Exim بیان شده است.

۲ فعال‌سازی ارتباطات SSL/TLS

برای پیکربندی SSL/TLS و استفاده از این پروتکل ابتدا باید گواهی‌نامه دیجیتال مربوطه را از مراکز صدور گواهی (CA)[۱] معتبر دریافت کرد (یا گواهی خود-امضا را تولید کرد). گرفتن گواهی دارای مراحلی است که برای اطلاعات بیشتر در این زمینه می‌توانید به گزارش ارائه شده توسط پژوهشکده آپای دانشگاه صنعتی امیرکبیر که در آدرس زیر قرار دارد مراجعه کنید:

http://apa.aut.ac.ir/?p=971

در ادامه این بخش، قصد داریم تا مراحل نصب گواهی و استفاده از ارتباطات امن را در Exim بیان کنیم:

فایل پیکربندی Exim در مسیر زیر قرار دارد که تغییرات مربوطه باید در آن داده شود. توصیه می‌شود قبل از تغییر این فایل، یک نسخه پشتیبان از آن تهیه کنید.

- /etc/exim.conf

توجه: به منظور اعمال تغییرات انجام شده در این فایل، باید با دستور زیر Exim را راه‌اندازی مجدد کرد.

```
service exim restart
```

برای استفاده از SSL/TLS باید مسیر گواهی‌نامه سرویس‌دهنده و کلید خصوصی به صورت زیر به Exim داده شود.

```
tls_certificate = /etc/exim.cert
tls_privatekey = /etc/exim.key
```

فایل گواهی (exim.cert)، یک موجودیت عمومی (غیر محرمانه) است ولی فایل کلید (exim.key) به صورت محرمانه باید نگهداری شود. توجه کنید که امکان دارد گواهی و کلید خصوصی هر دو در یک فایل باشند که به صورت زیر بیان می‌شود و با این وجود باز هم فقط گواهی به سرویس‌گیرنده ارسال خواهد شد.

زمانی که از یک مراکز صدور گواهی میانی، گواهی دریافت کنید، آن CA، زنجیره گواهی‌های میانی خود را در قالب یک بسته[۲] در اختیار شما قرار می‌دهد که باید به صورت زیر در فایل پیکربندی Exim قرار گیرد:

```
tls_verify_certificates = /etc/exim.cacert
```

[۱] Certificate Authority
[۲] Bundle

مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها و حوادث امنیتی سایبری)
تهران - بالاتر از چهارراه ولیعصر - نبش کوچه بالاور – ساختمان معاونت پژوهشی دانشگاه صنعتی امیرکبیر - طبقه سوم
کد پستی: ۱۵۹۱۶۳۴۳۱۱ تلفکس: ۶۶۴۶۰۳۰۸ Web: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir

۳ پیکربندی امن پروتکل SSL/TLS

در این بخش چگونگی پیکربندی امن SSL/TLS را در سرویس‌دهنده Exim بیان می‌کنیم. مواردی همچون به‌روزرسانی OpenSSL به آخرین نسخه به منظور کاهش حملاتی شبیه به خونریزی قلبی[۱]، استثنا کردن برخی الگوریتم‌های رمز به منظور کاهش حملاتی شبیه به FREAK، CRIME و LogJAM، غیرفعال سازی نسخه‌های ناامن SSL، برقرار کردن رمزنگاری‌های قوی که از Forward Secrecy (FS) پشتیبانی می‌کنند و فعال سازی HSTS را بیان می‌کنیم.

برای بررسی وضعیت امنیتی پروتکل SSL/TLS سرویس‌دهنده خود، می‌توانید به ابزاری که بدین منظور توسط پژوهشکده آپای دانشگاه صنعتی امیرکبیر طراحی شده و در آدرس زیر قرار دارد، مراجعه کنید.

https://sslcheck.certcc.ir

۳–۱ امن سازی پارامترهای دیفی هلمن

ما نیاز داریم تا یک پارامتر دیفی هلمن قوی را تولید کنیم، که می‌توانیم با دستور زیر این کار را انجام دهیم:

```
cd /etc/ssl/certs
openssl dhparam -out dhparam.pem 4096
```

و سپس باید به Exim بگوییم که از این پارامترها برای تغییر کلید دیفی هلمن[۲] استفاده کند:

```
tls_dhparam = /etc/ssl/certs/dhparam.pem
```

۳–۲ غیرفعال سازی الگوریتم‌های رمزنگاری ضعیف

Forward Secrecy اطمینان می‌دهد که صحت[۳] یک کلید جلسه[۴] حتی وقتی که کلیدهای زیادی مورد مخاطره قرار گرفتند، حفظ می‌شود. FS کامل[۵] این مورد را با استخراج یک کلید جدید برای هر جلسه، به انجام می‌رساند. این بدان معناست که زمانی که کلید خصوصی به مخاطره افتاد، نمی‌تواند برای رمزگشایی ترافیک SSL مورد استفاده قرار گیرد.

پیشنهاد می‌شود دستور زیر را برای استفاده از الگوریتم‌های رمزنگاری قوی و غیرفعال سازی رمزنگاری‌های ضعیف در فایل پیکربندی وارد کنید.

```
tls_require_ciphers = ALL:-SSLv3:RC4:-SSLv2:!ADH:+HIGH:+MEDIUM:-LOW:-EXP
```

---

[۱] Heartbleed
[۲] DHE key-exchange
[۳] Integrity
[۴] Session Key
[۵] Perfect Forward Secrecy

مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها و حوادث امنیتی سایبری)
تهران - بالاتر از چهارراه ولیعصر - نبش کوچه بالاور – ساختمان معاونت پژوهشی دانشگاه صنعتی امیرکبیر - طبقه سوم
کد پستی: ۱۵۹۱۶۳۴۳۱۱ تلفکس: ۶۶۴۶۰۳۰۸ Web: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir

۳-۳ غیرفعال سازی SSLv2 و SSLv3

SSLv2 و SSLv3 (به خاطر حمله POODLE) ناامن هستند و باید غیرفعال شوند. برای غیرفعال سازی آنها، فایل مخصوص پیکربندی را به صورت زیر ویرایش می‌کنیم:

```
openssl_options = +no_sslv2 +no_sslv3
```

۴ منابع

1 https://help.directadmin.com/item.php?id=598

2 https://www.ndchost.com/wiki/cpanel/poodle-fix

3 http://www.exim.org/exim-html-current/doc/html/spec_html/index.html

4 http://www.exim.org/exim-html-current/doc/html/spec_html/index.html

5 https://help.directadmin.com/item.php?id=598

6 http://www.exim.org/exim-html-current/doc/html/spec_html/ch-encrypted_smtp_connections_using_tlsssl.html

مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها و حوادث امنیتی سایبری)
تهران - بالاتر از چهارراه ولیعصر - نبش کوچه بالاور – ساختمان معاونت پژوهشی دانشگاه صنعتی امیرکبیر - طبقه سوم
کد پستی: ۱۵۹۱۶۳۴۳۱۱ تلفکس: ۶۶۴۶۰۳۰۸ Web: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir