راه‌اندازی و پیکربندی امن پروتکل SSL/TLS بر روی سرویس‌دهنده پست الکترونیک Zarafa 7

شماره مستند APA-AMIRKABIR-13950703-1

تاریخ نگارش ..... ۳ مهر ۱۳۹۵

شماره نگارش ۱/۰

نگارش ..... آپای امیرکبیر

طبقه‌بندی ..... عادی

فهرست مطالب

۱ مقدمه ۱

۲ فعال‌سازی ارتباطات HTTPS ۲

۲-۱ فعال سازی SSL برای پروتکل IMAP ۲

۳ پیکربندی امن پروتکل SSL/TLS ۴

۳-۱ غیر فعال کردن SSLv2 و SSLv3 ..... ۴

۳-۲ غیر فعال کردن الگوریتم‌های رمزنگاری ضعیف ۴

۴ منابع ۶

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 بر روی سرویس‌دهنده پست الکترونیک Zarafa نسخه ۷,۱,۱۱ را بیان می‌کنیم.

۲ فعال‌سازی ارتباطات HTTPS

برای پیکربندی سرویس‌دهنده HTTPS 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 را در Zarafa بیان کنیم:

۱. در ابتدا با ترکیب فایل کلید (star_domain_com.key) و گواهی اصلی مربوط به دامنه خودتان (star_domain_com.crt)، فایل star_domain_com.pem را مطابق زیر ایجاد کنید:

```
cat /path/to/star_domain_com.key /path/to/star_domain_com.crt >
/path/to/star_domain_com.pem
```

۲. فایل‌های star_domain_com.pem و ca.crt (زنجیره گواهی‌های میانی‌ای که از مرکز صدور گواهی دریافت کرده‌اید) را به سرور Zarafa انتقال دهید.

۳. تنظیمات SSL را در فایل server.cfg مطابق زیر انجام دهید.

پورت ۲۳۷ برای ارتباطات SSL در نظر گرفته شده است که در صورت لزوم می‌توانید آن را تغییر دهید.

```
server_ssl_enabled      = yes
server_ssl_port         = 237
server_ssl_key_file     = /path/to/star_domain_com.pem
server_ssl_key_pass     =
server_ssl_ca_file      = /path/to/ca.crt
```

۴. سرویس‌دهنده zarafa را راه‌اندازی مجدد کنید.

۲–۱ فعال سازی SSL برای پروتکل IMAP

۱. فایل پیکربندی را با دستور زیر باز کنید.

```
vi /etc/zarafa/gateway.cfg
```

۲. تنظیمات را به صورت زیر انجام دهید.

```
# enable/disable IMAP, and IMAP listen port
imap_enable    =    yes
```

[۱] Certificate Authority

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

```
imap_port       =       143
# enable/disable Secure IMAP, and Secure IMAP listen port
imaps_enable = yes
imaps_port = 993
# File with RSA key for SSL
ssl_private_key_file = /etc/zarafa/privkey.pem
#File with certificate for SSL
ssl_certificate_file = /etc/zarafa/cert.pem
```


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 پروتکل SSL/TLS را در سرویس‌دهنده پست الکترونیک Zarafa بیان می‌کنیم. مواردی همچون استثنا کردن برخی الگوریتم‌های رمزنگاری به منظور کاهش حملاتی شبیه به FREAK، CRIME و LogJAM، غیرفعال سازی نسخه‌های ناامن SSL و برقرار کردن رمزنگاری‌های قوی که از Forward Secrecy (FS) پشتیبانی می‌کنند را در این بخش 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 غیر فعال کردن SSLv2 و SSLv3

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

1. /etc/zarafa/server.cfg

```
server_ssl_protocols = !SSLv2 !SSLv3
```

2. /etc/zarafa/gateway.cfg

```
ssl_protocols = !SSLv2 !SSLv3
```

۳–۲ غیر فعال کردن الگوریتم‌های رمزنگاری ضعیف

پیشنهاد می‌شود دستور زیر را برای استفاده از الگوریتم‌های رمزنگاری قوی و غیرفعال سازی رمزنگاری‌های ضعیف در فایل پیکربندی وارد کنید. اگر نسخه OpenSSL شما قدیمی باشد، الگوریتم‌های غیرقابل دسترس به صورت خودکار دور انداخته می‌شوند. دقت کنید که همیشه از کل الگوریتم‌ها استفاده کنید و اجازه دهید تا OpenSSL، آنهایی را که پشتیبانی می‌کند، انتخاب کند.

1. /etc/zarafa/server.cfg

```
server_ssl_ciphers = ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-
GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-
SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-
SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-
SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-
SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-
AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-
SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-
SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA:AES256-
SHA:AES:CAMELLIA:DES-CBC3-
SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK:!aECDH:!EDH-DSS-DES-CBC3-
SHA:!EDH-RSA-DES-CBC3-SHA:!KRB5-DES-CBC3-SHA
```

```
server_ssl_prefer_server_ciphers = yes
```

2. /etc/zarafa/gateway.cfg

```
ssl_ciphers = ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-
SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-
RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-
AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-
ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-
SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-
SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-
SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:AES128-GCM-SHA256:AES256-
GCM-SHA384:AES128-SHA:AES256-SHA:AES:CAMELLIA:DES-CBC3-
SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK:!aECDH:!EDH-DSS-DES-CBC3-
SHA:!EDH-RSA-DES-CBC3-SHA:!KRB5-DES-CBC3-SHA
ssl_prefer_server_ciphers = yes
```

توجه: برای اعمال تغییرات انجام شده در فایل‌های مورد نظر، باید سرویس‌های مربوطه را راه‌اندازی مجدد کرد.

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

۴ منابع

1. http://wiki.zarafa.com/index.php/Zarafa_with_official_SSL_certificates
2. https://doc.zarafa.com/trunk/Administrator_Manual/en-US/html/_ssl_connections_and_certificates.html
3. http://die-krueger.de/?qa_faqs=enable-imap-ssl-for-zarafa
4. https://lists.fedoraproject.org/pipermail/zarafa-announce/2014-October/000058.html