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

شماره مستند APA-AMIRKABIR-13950710-1

تاریخ نگارش ..... ۱۰ مهر ۱۳۹۵

شماره نگارش ۱/۰

نگارش ..... آپای امیرکبیر

طبقه‌بندی ..... عادی

فهرست مطالب

۱ مقدمه

شرکت‌ها و سازمان‌های کوچک عمدتاً از شرکت‌های سرویس‌دهنده Hosting برای پست الکترونیک خود استفاده می‌کنند اما شرکت‌های متوسط و بزرگ به دلیل مسائل امنیتی و حساسیت سرویس پست الکترونیک برای آنان، ناچار به استفاده از یک Mail Server اختصاصی در محل خود هستند.

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، راه‌اندازی و پیکربندی امن پروتکل SSL/TLS بر روی سرویس‌دهنده پست الکترونیک Axigen بیان شده است.

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 این قسمت ابتدا چگونگی تنظیمات مربوط به گوش دادن روی پورت‌های مختلف (برای سرویس‌های مختلف) و روش نصب گواهی‌نامه SSL را توضیح می‌دهیم.

برای تخصیص دادن پورت‌ها به سرویس‌های مورد نظر (به منظور استفاده از ارتباطات امن) ابتدا وارد حساب کاربری Webadmin شوید (از طریق http://127.0.0.1:9000) و سپس به مسیر زیر بروید:

Webadmin -> Services -> specific service

و سپس مراحل زیر را انجام دهید:

۱. روی دکمه 'Add listener' کلیک کنید.
۲. IP و پورت (مطابق لیست زیر) مربوطه که قرار است روی آن گوش فرا داده شود را وارد کنید.

993 IMAPS 995 POP3S 465 SMTPS 443 HTTPS

۳. روی دکمه 'Quick Add' کلیک کنید.
۴. روی دکمه 'Edit' کلیک کنید.
۵. به قسمت 'SSL Settings' بروید.
۶. ویژگی 'Enable SSL for this listener' را بررسی کنید.
۷. مسیر فایل گواهی‌نامه را در قسمت مربوطه وارد کنید. فایل گواهی (پیش‌فرض) در سیستم‌عامل‌های مختلف در مسیرهای زیر قرار دارد:

- *'/var/opt/axigen/axigen_cert.pem'* for Linux and Solaris
- *'/var/axigen/axigen_cert.pem'* for BSD
- *'C:\Program Files\Axigen Mail Server\axigen_cert.pem'* for Windows

۸. در نهایت روی دکمه 'Save Configuration' کلیک کنید.

[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

۳ پیکربندی امن پروتکل SSL/TLS

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

پیش از شروع امن‌سازی و پس از آن، از سرویس زیر برای ارزیابی وضعیت امنیتی SSL/TLS در سرویس دهنده خود استفاده نمایید تا اطمینان حاصل کنید که وضعیت امنیتی سرویس‌دهنده ارتقا یافته است.

https://sslcheck.certcc.ir

۳–۱ غیرفعال سازی SSLv2 و SSLv3

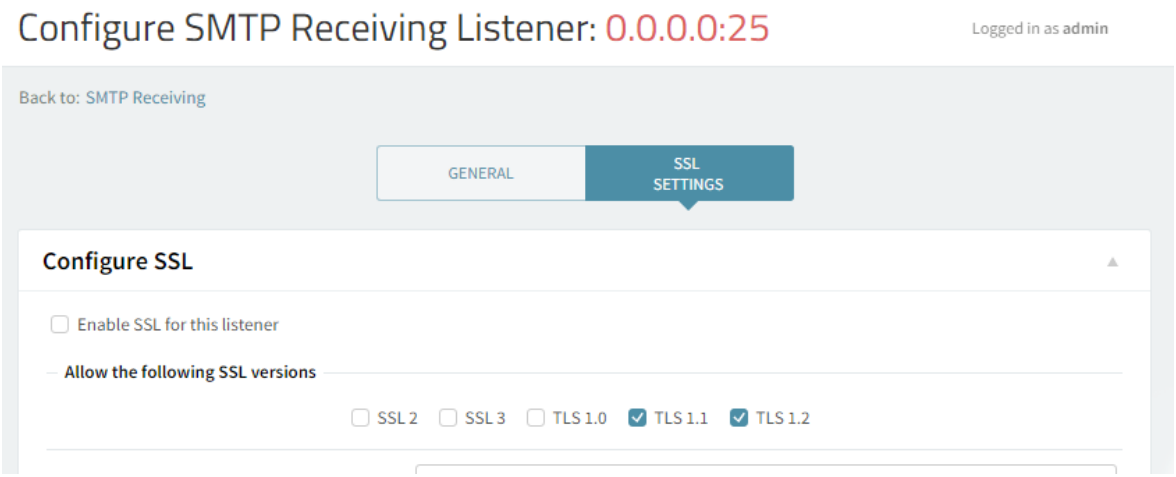
SSLv2 و SSLv3 (به خاطر حملاتی مثل POODLE) ناامن هستند و باید غیرفعال شوند. برای غیرفعال سازی آنها، ابتدا وارد حساب کاربری Webadmin شوید و مراحل زیر را انجام دهید:

۱. به مسیر زیر بروید:

Webadmin -> Services -> specific service

۲. روی دکمه 'Edit' از سرویس مورد نظر کلیک کنید.

۳. به قسمت 'SSL Settings' بروید. در اینجا می‌توانید نسخه‌های ناامن SSL را برای سرویس‌های مورد نظر، غیر فعال کنید.



۳–۲ غیرفعال سازی الگوریتم‌های رمزنگاری ضعیف

Forward Secrecy اطمینان می‌دهد که صحت[۱] یک کلید جلسه[۲] حتی وقتی که کلیدهای زیادی مورد مخاطره قرار گرفتند، حفظ می‌شود. FS کامل[۳] 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 مراحل زیر را برای استفاده از الگوریتم‌های رمزنگاری قوی و غیرفعال سازی رمزنگاری‌های ضعیف، انجام دهید.

برای این کار، ابتدا وارد حساب کاربری Webadmin شوید و مراحل زیر را انجام دهید:

۱. به مسیر زیر بروید:

Webadmin -> Services -> specific service

۲. روی دکمه 'Edit' از سرویس مورد نظر کلیک کنید.

۳. به قسمت 'SSL Settings' بروید و عبارت زیر را در قسمت 'Use Cipher suite' قرار دهید.

```
!AECDH:!ADH:!aNULL:!eNULL:!RC4:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH:!MD5:!EDH:!EXPORT
```

توجه: اگه گزینه مربوط به "ترتیب الگوریتم‌ها" را علامت بزنید، الگوریتم‌ها به ترتیب آنچه که شما وارد کرده‌اید انتخاب خواهد شد.

۳–۳ 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:

```
openssl dhparam -out dhparam.pem 4096
```

و سپس باید به Axigen بگوییم که از این پارامترها برای تغییر کلید دیفی هلمن[۴] استفاده کند.

برای این کار، مراحل زیر را انجام دهید:

۱. ابتدا وارد حساب کاربری Webadmin شوید و به مسیر زیر بروید:

Webadmin -> Services -> specific service

۲. روی دکمه 'Edit' از سرویس مورد نظر کلیک کنید.

---

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

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

به قسمت 'SSL Settings' بروید و در قسمت ’path to DH parameter file‘، مسیر مربوط به پارامترهای دیفی هلمن که در بالا ساختید را وارد کنید.

۴ منابع

1 https://www.axigen.com/documentation/index.php/The_Axigen_WebAdmin_Service_-_Admin_Manual

2 https://www.axigen.com/knowledgebase/How-to-configure-SSL-settings_213.html

3 https://www.axigen.com/documentation/index.php/Advanced_Configuration_of_Axigen_-_Admin_Manual

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