Array Networks Blog

16 DEC, 15

0 COMMENT

How Safe Is OpenSSL? Part III: Best Practices

POSTED IN ADC, APPLICATION DELIVERY CONTROLLERS, SERVER LOAD BALANCING, SSL VPN, VIRTUALIZED ADC BY PAUL ANDERSEN

Tweet Share Share 0 print

In parts I and II of this blog series, we examined the frequency and severity of OpenSSL vulnerabilities, and key differences between OpenSSL and Array's proprietary SSL stack. In this final edition of the series, we've promised to provide useful tips and techniques as well as best practices to help you use SSL while mitigating risk.

Network security as a whole has come under increasing scrutiny in the past year, as jaw-dropping security breaches exposed confidential information including social security numbers, passwords, credit card information and more. In addition, several high-profile network vulnerabilities have been reported that have made global headlines.

It's now fairly common for network security managers to be called upon to report to their respective organization's board of directors – and they want assurances that their company won't be the star of the next big breach headline.

Luckily, there are a number of strategic (and tactical) steps you can take to minimize risk and maintain a strong security posture. To name just a few, in no particular order:

Identify if and where OpenSSL resides in your network. You'll need to ask your vendors, but it's very commonly used for Web servers (estimates range from 50 to 75% worldwide), and it's also common in SSL VPN appliances and application delivery controllers, among other products. OpenSSL may also be used in 'non-production' applications for some products – for example, Array uses OpenSSL for our WebUI, XML RPC and SOAP APIs in our APV Series application delivery controllers. All production traffic, however, runs over our proprietary SSL stack.

Know which version(s) of OpenSSL are in use. In part I of this series, we determined that older versions of OpenSSL may be generally safer – though that's not always true. The flawed code that was responsible for the Heartbleed bug, for example, was introduced into the code ***two years*** before researchers discovered the vulnerability. (And for the record, the version of OpenSSL that Array uses for non-production traffic predates the introduction of the Heartbleed flaw.)

Consider a layered security approach. If OpenSSL is running on your Web or application servers, consider adding application delivery controllers that run a proprietary SSL stack – like Array's APV Series – to load balance traffic among servers. You'll gain in performance, availability and flexibility, while protecting the servers through a reverse-proxy architecture, kernel-level ACLs, packet filtering, DDoS protection and WebWall application security suite. This strategy effectively 'walls off' OpenSSL-based servers behind non-OpenSSL appliances.

Rethink security for remote and mobile workers. A number of reported OpenSSL vulnerabilities over the years have had the potential to allow man-in-the-middle (MitM) attacks – however, SSL VPNs are one of the most frequently mentioned methods of preventing MitM exploits for remote and mobile workers who need to access the corporate network. Therein lies the conundrum – if your SSL VPN appliance is based upon OpenSSL, but OpenSSL has had multiple MiTM vulnerabilities.. Enough said. Read about Array's secure access gateways (SSL VPNs), which are also based upon Array's proprietary SSL stack. Another strategy you may wish to consider is remote desktop protocol (RDP) for remote/mobile workers. Array's DesktopDirect feature set for the AG Series can significantly mitigate data leakage by ensuring that data never resides on the remote device – it remains on the corporate network at all times.

Reexamine your authentication schema. Many of the previous OpenSSL vulnerabilities have had the potential to expose users' passwords. If you're following best practices of requiring strong passwords, and requiring users to change them frequently, that's all to the good. However, some SSL VPN products (like Array's) offer additional authentication checks that can be used to further bolster security. For example, in addition to passwords you might also authenticate the device MAC address or hardware ID.

Another option is two-factor authentication. Array has partnered with a number of third-party vendors of this technology, who offer cloud-based, virtual or dedicated solutions. Typically the technology pairs something you know (i.e. your password) with something you have (a token or smart device app with constantly changing access codes, which are synchronized with the AG Series SSL VPN appliance).

Of necessity, the list above is focused on the technology area that Array does best: application delivery networking. A search on 'protect against Heartbleed' or other well known OpenSSL vulnerabilities will also yield dozens of articles that offer other viewpoints. Are there other strategies and tactics that you've developed to mitigate risk while using OpenSSL-based servers and networking products? Join the conversation by commenting below.

Stay Connected

Subscribe by Email

E-mail

unsubscribe

Submit

Latest Tweets

Array's Management Platform (AMP) latest release offers new enhancements. AMP provides centralized #configuration,... https://t.co/VV5a54c4WJ
6 months ago

Using a #virtual #appliance to process traffic is a key #encryption strategy #enterprises can use to improve... https://t.co/okBrz2HxCf
6 months ago

@Interop attendees...Swing by booth 325 to see how to supercharge software-based #WAF & #NGFW solutions w/ Array's... https://t.co/2Vyu7sf5Cj
6 months ago

RT @cegasecurity: @ArrayNetworks y @CEGASecurity, estarán exhibiendo la #AVXSeries y otras #tecnologías de #ciberseguridad en... https://t.co/kCHUJznxC3
6 months ago

We are ready for the @Interop event! Come see us in booth 325 to learn more about our #NetworkFunctionsPlatform fo... https://t.co/s1edy5wWDU
6 months ago