Array Networks Blog

26
AUG, 15

How Safe Is OpenSSL? Part I

POSTED IN APPLICATION DELIVERY CONTROLLERS, SSL VPN BY PAUL ANDERSEN

0
COMMENT

Tweet Share Share 0 print

The passing of the one-year anniversary of the OpenSSL Heartbleed vulnerability – and a recent rash of highly exploitable vulnerabilities with names of lesser cachet – led me to wonder: Just how frequently are OpenSSL vulnerabilities reported, and what are their impacts?

While Array has developed our own proprietary SSL stack for production traffic, we do use OpenSSL for certain of our products' functions such as our XML RPC and SOAP APIs, WebUIs and other non-traffic-related tasks. Thus, this exercise is categorically not about OpenSSL bashing – rather, it's intended to gain a better understanding of the vulnerability landscape and to serve as a foundation for discussion on network security as a whole.

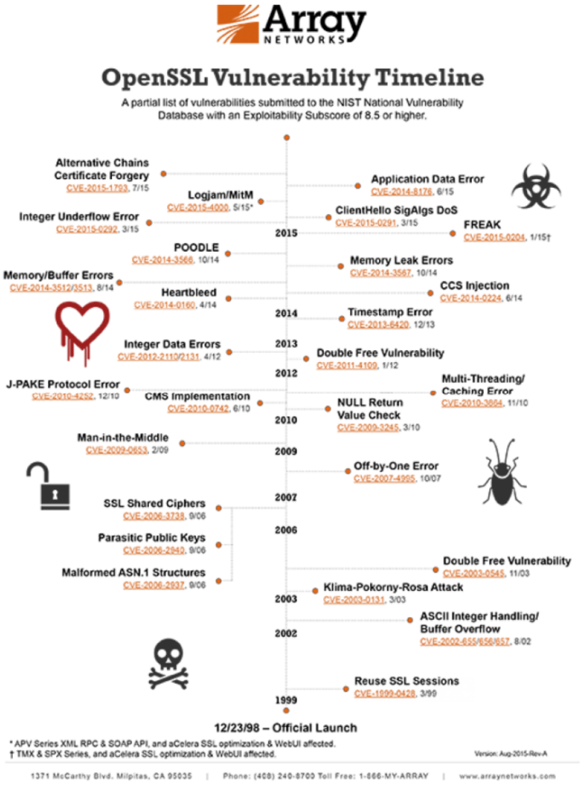
The infographic below was compiled from the NIST National Vulnerability Database, and lists vulnerabilities with Exploitability Subscores of 8.5 and higher (with 10 being the highest). While every attempt was made to ensure accuracy and completeness, the vast scope of the NIST database makes this a nearly insurmountable task.

As you will see, like almost every software ever created, OpenSSL has had its share of vulnerabilities over the years. Many were reported at or shortly after a major product release; after the 1.0.2 release on Jan. 22, 2015, for example, CVE-2015-0291 and CVE-2015-0292 were reported less than two months later.

In many ways, that's the nature of the beast in open-source software development. The very structure that gives open source such great qualities – multiple developers (often volunteers) working together to create a freely-available code base – can also lead to errors because developers are working independently. However, with an entire community of developers, any errors are typically fixed very quickly, thus mitigating the impact.

And in all fairness, Array products were vulnerable to a couple of the vulnerabilities listed here, as well as a handful of others with lesser exploitability scores. Usually those vulnerabilities were related to the functions mentioned above, or to our older, end-of-sale products like the SPX and TMX Series. Follow the Array Support Twitter feed to keep up to date on all our product notifications.

In Part II of this blog series, I'll dig deeper into the differences between open-source development and proprietary code bases, and offer concrete suggestions on keeping your network safe. Until then, let's all be careful out there.


Array NETWORKS

OpenSSL Vulnerability Timeline

A partial list of vulnerabilities submitted to the NIST National Vulnerability Database with an Exploitability Subscore of 8.5 or higher.

* APV Series XML RPC & SOAP API, and aCelera SSL optimization & WebUI affected.
† TMX & SPX Series, and aCelera SSL optimization & WebUI affected.

Version: Aug-2015-Rev-A

1371 McCarthy Blvd. Milpitas, CA 95035 | Phone: (408) 240-8700 Toll Free: 1-866-MY-ARRAY | www.arraynetworks.com

Application Delivery Controllers heartbleed OpenSSL shellshock SSL VPN vulnerabilities

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

Tag Cloud

aCelera ADCs

application delivery controller

Application Delivery Controllers

AVX10650 BYOD

BYOD Policy DesktopDirect

Global Server Load Balancing