RAPID RESPONSE
Confidential | Do Not Distribute

RAPID RESPONSE

OpenSSL Security Advisory Issued June 5, 2014

Summary Description

On June 5, 2014, the OpenSSL Project issued a security advisory describing six exploits within OpenSSL code. Of the six vulnerabilities outlined by OpenSSL, A10 is only vulnerable to the MITM ChangeCipherSpec (CCS) Injection flaw (CVE-2014-0224). A10 Thunder or AX ADCs are vulnerable under specific conditions described below. The vulnerability can be immediately mitigated through server updates, and A10 will be issuing a patch to secure A10 ADC and TPS platforms. Timing and details for the patch follow.

Vulnerability Assessment

Affected Platforms: *Thunder and AX ADC series, Thunder TPS Series*

Affected Software Versions: *ACOS versions 2.6.1-GR1-x, 2.7.X, 3.0.0 (TPS)*

The A10 Thunder and AX Application Delivery Controllers (ADC) are vulnerable to **CVE-2014-0224-** SSL/TLS Man-in-the-Middle attack. The vulnerability is limited to deployments where the Thunder or AX device is acting like an SSL client and is connecting to a back-end server that is running OpenSSL 1.0.1 or 1.0.2-beta1. For example, if a Thunder or AX ADC is terminating SSL traffic and re-encrypting the traffic before sending it to a back-end server—a server-side SSL deployment configured as "server-ssl" under the HTTPS virtual port for ADC solution — then the devices will be susceptible to the Man-in-the-Middle attack. In addition, if a Thunder or AX ADC is configured for SSL intercept as an SSL forward proxy using the "forward-proxy-enable" command, then it is also vulnerable.

Exposure on all Thunder and AX platforms is limited, as most SSL ADC deployments are configured for SSL offload and not for SSL re-encryption (server-side SSL).

With Thunder TPS, only the Web GUI is vulnerable to the MITM flaw.

There is limited vulnerability with EX and ID series products.
We will be documenting vulnerabilities and mitigation recommendations shortly.

Thunder series SSL management interface (Web GUI) is not vulnerable.

Affected ADC Configurations (highlights denote specific configuration issues)

A10 Software defect 187969 has been filed to document the exploit.

ADC Server-side Deployment:

```
slb template server-ssl server-encryption

!

slb virtual-server vip 10.10.10.10

  port 443  https

    source-nat pool nat

    service-group sg101

    template client-ssl client-encryption

    template server-ssl server-encryption
```

Client side (client-ssl) SSL connections are not vulnerable to this exploit.

For SSL Intercept Deployment:

```
slb template client-ssl test

  forward-proxy-enable

  forward-proxy-ca-cert testca

  forward-proxy-ca-key testca

!

slb virtual-server vip1 0.0.0.0 acl 101

  port 443  https

    name _wildcard_v4_101_HTTPS_443

    service-group rs8080

    template client-ssl test

    no-dest-nat port-translation
```

Mitigation Recommendations

A10 Networks will be releasing patch(s) on Wednesday, June 11, 2014 by the end of the business day. A10 recommends that customers upgrade all A10 Thunder or AX series products when the patch is available.

A10 will issue patches for the following versions of ACOS:

- 2.6.1-GR1-P12-SP1
- 2.7.0-P6-SP2
- 2.7.1-P5-SP2
- 2.7.2-P1-SP1
- 3.0.0-tps-p1-sp1

As an immediate mitigation step, customers can upgrade vulnerable back-end servers to the patched OpenSSL server version.

Additional Resources

OpenSSL Advisory
https://www.openssl.org/news/secadv_20140605.txt

CVE Database
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224

A10 products are NOT AFFECTED by these vulnerability advisories issued by OpenSSL on June 5, 2014:

- CVE-2014-0221, DTLS recursion flaw
- CVE-2014-0195, DTLS invalid fragment vulnerability
- CVE-2014-0198, SSL_MODE_RELEASE_BUFFERS NULL pointer dereference
- CVE-2010-5298, SSL_MODE_RELEASE_BUFFERS session injection or denial of service
- CVE-2014-3470, Anonymous ECDH denial of service