SECURITY ADVISORY

#Multiple OpenSSL vulnerabilities published on March 8th and 19th, 2015

Summary Description

This is a combined vulnerability advisory covering a number of patches that OpenSSL released on March 8th and 19th. While most of the vulnerabilities do not affect A10 products, A10 Networks is issuing an advisory to clarify the implications for A10 customer in particular due to the conflicting information in the media. This security advisory addresses the following CVEs:

- CVE-2015-0290 – Multi-block corrupted pointer
- CVE-2015-0291 - OpenSSL 1.0.2 ClientHello sigalgs DoS
- CVE-2015-0204 - RSA silently downgrades to EXPORT_RSA [Client] (aka FREAK)
- CVE-2015-0286 – Segmentation fault in ASN1_TYPE_cmp
- CVE-2015-0292 – Base64 decode
- CVE-2015-0209 – Use After Free following d2i_ECPrivatekey error
- CVE-2014-3571 - DTLS segmentation fault in dtls1_get_record
- CVE-2015-0206 – DTLS memory leak in dtls1_buffer_record
- CVE-2015-0207 – Segmentation fault in DTLSv1_listen

Details as Pertaining to A10 Software and Equipment

A10 engineering analyzed the code base with regards to the “high” and “moderate” vulnerabilities and reached the following conclusions.

CVE-2015-0290 and •CVE-2015-0291

- CVE-2015-0290 – Multi-block corrupted pointer
- CVE-2015-0291 - OpenSSL 1.0.2 ClientHello sigalgs DoS

CVE-2015-0290 and CVE-2015-0291 only affect OpenSSL version 1.0.2 and none of the current A10 software base includes this OpenSSL version.

CVE-2015-0204

CVE-2015-0204 - RSA silently downgrades to EXPORT_RSA [Client] (aka FREAK)

On January 8th, OpenSSL announced a vulnerability which only affects the client side of a connection due to silently accepting downgrade to RSA_EXPORT cipher.

This vulnerability solely affects the client side of a connection which is due to the client code allowing the server to degrade the RSA negotiation with proper length key to one with a low level (512 bit) by degrading to an export grade encryption.

During normal operation, if a server is contacted by a client that claims to only support RSA_EXPORT ciphers, the server will generate a 512 bit key and sign it with the “full length” key for that site so the client can authenticate. Depending on the implementation, this key may be generated only once at start time and be kept around for long time allowing a malicious third party to request it and crack it offline.

In essence, the vulnerability allows a malicious third party to perform a Man in the Middle (MITM) attack and intercept the traffic.

Note that in order for this attack to succeed, a number of prerequisites need to be met:

1. The server needs to supply a low grade key – be it automatically generated or manually installed.
2. The client needs to be vulnerable to CVE-2015-0204 (FREAK).

When discussing FREAK in an ACOS context, there are two attack surfaces – ACOS being the server and ACOS being the client.

Server-side

Since this is solely a client-side bug, ACOS is inherently not vulnerable when terminating connections.

Furthermore, as a design choice, we have decided to not allow for automatic generation of low grade keys which means that clients that are talking to services fronted by ACOS devices will not be exploitable in the context of those services, unless the certificate is also deployed to lower grade security devices that would generate valid, low grade key.

Client-side

In some particular configurations like SSL termination and re-encryption, the ACOS device will serve as a client after re-encrypting the traffic and there is potential for exploitation if the aforementioned conditions are met.

In the case of SSL termination on a load balancer and re-encryption to a backend server, the risk is limited to the network and devices between the load balancers and the servers.

In the SSL Insight case, the risk is greater and if the target server supports key downgrade, it may be exploitable.

Initially the CVE was classified as “low severity”. On January 19th, it was reclassified to “high severity”. Per OpenSSL this reclassification is solely based on the number of systems affected and does not have a technical merit and does not increase the risk to ACOS devices.

CVE-2015-0286, CVE-2015-0292 and CVE-2015-0209

- CVE-2015-0286 – Segmentation fault in ASN1_TYPE_cmp
- CVE-2015-0292 – Base64 decode
- CVE-2015-0289 – PKCS7 NULL pointer dereferences
- CVE-2015-0209 – Use After Free following d2i_ECPrivatekey error

ACOS does include vulnerable code and it is executed under different circumstances. Due to the negligible severity and the prerequisites necessary to exploit those vulnerabilities, they are considered low risk. In particular CVE-2015-0289 and CVE-2015-0292 require the user to be an administrator in order to be triggered.

Updates for those software defects will be provided as a part of the regular update cycle.

CVE-2015-0206, CVE-2014-3571 and CVE-2015-0207

- CVE-2014-3571 - DTLS segmentation fault in dtls1_get_record
- CVE-2015-0206 – DTLS memory leak in dtls1_buffer_record
- CVE-2015-0207 – Segmentation fault in DTLSv1_listen

Currently ACOS does not support DTLS and none of those vulnerabilities are applicable.

Vulnerability Assessment

Affected Platforms: *ADC, CGN, TPS*

Affected Software Versions: *2.6.1-GR1-X, 2.7.X, TPS 3.x.x.*

Mitigation Recommendations

In the case of CVE-2015-0204 it is recommended that the user disable the export ciphers on the client side. This can be done by creating a template enumerating the ciphers to be used like in the following example (details would be platform specific).

```
slb template cipher cipher_list
 SSL3_RSA_DES_192_CBC3_SHA
…
TLS1_RSA_AES_256_SHA256
slb template server-ssl server_template
cert device
key device
template cipher cipher_list
```

In addition, if the use case is only re-encryption of traffic to the backend server over a trusted network, it is recommended that the risk is evaluated before any additional action is taken.

Software Updates

Software updates resolving this potential vulnerability will be published at the following URL when available:

http://www.a10networks.com/support-axseries/downloads/downloads.php

The following table summarizes update versions resolving all of the above CVEs.

Vulnerable Release	Resolved Release
3.1.0-P1	3.2.0
2.6.1-GR1-P14	2.6.1-GR1-P15
2.7.0-P6	2.7.0-P7
2.7.1-P6	2.7.1-GR1
2.7.2-P4	2.7.2-P5
4.0.0	4.0.1

The following table summarizes update versions resolving CVE-2015-0204 (FREAK).

Vulnerable Release	Resolved Release
3.1.0-P1	3.1.1
2.6.1-GR1-P14	2.6.1-GR1-P15
2.7.0-P6	2.7.0-P7
2.7.1-P6	2.7.1-GR1
2.7.2-P4	2.7.2-P5
4.0.0	4.0.1

References

1. OpenSSL Security Advisory – 2015-03-08: https://www.openssl.org/news/secadv_20150108.txt
2. OpenSSL Security Advisory – 2015-03-19: https://www.openssl.org/news/secadv_20150319.txt