RAPID RESPONSE

SECURITY ADVISORY

"POODLE" #CVE-2014-3566 published on Oct. 14, 2014

UPDATED November 3 with these changes: • In the "aFlex rule to redirect all SSL v3 clients to an upgrade page" code, the script was updated (the previous script did not cover all cases). • In the "aFlex rules for dropping all SSL v3 requests" code, the script was updated (the previous script did not cover all cases).

UPDATED October 22 with these changes: • CGN was removed from "Patch Information" table; not applicable • "Using aFleX" section was updated to include performance impact information • In the "aFlex rule to redirect all SSL v3 clients to an upgrade page" code, "template1" is used in place of "pratap" • In the "aFlex rules for dropping all SSL v3 requests" code, "template1" is used in place of "pratap"

Summary Description

On October 14th, 2014, CVE-2014-3566 (http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3566) was published, revealing a design flaw in the SSL protocol version 3. The flaw is in the ability to downgrade to lower version of the protocol and the way the padding is handled, allowing an attacker to infer the value of a single byte from the stream. Repeated a number of times, it is possible that the attacker would be able to extract larger portions of the plain text message, which could contain sensitive authentication or other material. The attack is very similar to the BEAST attack from 2011 (http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3389), but requires much lower amount of upfront information.

Before the decryption attack is executed, it is necessary for the attacker to force the connection to downgrade the cipher to SSL v3. This is possible due to the ability to do in connection protocol downgrades, which has proven to be an issue in previous attacks of that sort.

In all cases, the attacker needs to be able to view and modify traffic on the network - which somewhat limits the ability to execute the attack.

This is a protocol flaw and is implementation independent and as a result, affects platforms from a large number of software and hardware vendors.

Details

On October 14th, 2014, in a post titled "This POODLE Bites: Exploiting TheSSL 3.0 Fallback" (URL: https://www.openssl.org/~bodo/ssl-poodle.pdf), researchers Bodo Möller, Thai Duong and Krzysztof Kotowicz from Google released a protocol flaw.

When dealing with exposure to a vulnerability, in the majority of the A10 platforms, we need to consider both the management and data planes separately.

The management plane for almost all A10 platforms is built with the FIPS compliant version the OpenSSL library, which does not support SSL v3, and as a result very few product lines are affected. Currently only TPS 2.9.1-p2 and 3.0.tps-p2-sp5 are affected; we are working on delivering patches based on OpenSSL 1.0.1j.

On the data plane, A10 devices support SSL v3 and it is possible for a third party to exploit that fact and downgrade a connection to SSL v3. A10 will be implementing the TLS_FALLBACK_SCSV patch in the next scheduled patch release. In the meantime, it is recommended that customers use the **disable sslv3** command (as described below) to prevent exploitation. If support for legacy clients is necessary, it is recommended that customers create a separate VIP to accommodate those legacy clients.

In addition to the ability to disable the protocol, A10 provides an example aFleX script that can redirect clients to a page explaining how to upgrade their clients.

Versions 2.6.x and 2.7.0 do not support the **disable sslv3** command. Customers of those versions are encouraged to upgrade to newer software trains or use the aFleX script provided below. In addition to that, A10 will provide backport of the **disable sslv3** command in version 2.6.1-GR1-P14 and 2.7.0-P7, correspondingly.

Vulnerability Assessment

Affected Platforms (management plane): *TPS*

Affected Platforms (data plane): *ADC, CGN, TPS, AX, ID, EX, aGalaxy, HVA*

Affected Software Versions: *ADC 2.6.1-GR1-x, 2.7.x, CGN 2.6.6-GR1-x, 2.8.x, TPS 2.9.1, 3.0*

Patch Information

SSL v3 is a protocol that has long been superseded by TLS1.0 and later 1.2. There is no particular need to use this protocol for management of A10 appliances.

Technology	Major Release	Fixed (TLS_FALLBACK_SCSV)	Backported "disable SSLv3"
ADC	2.6.1-GR1-P13	2.6.1-GR1-P14	2.6.1-GR1-P14
ADC	2.7.0-P6	2.7.0-P7	2.7.0-P7
ADC	2.7.1-P5	2.7.1-P7	n/a
ADC	2.7.2-P2	2.7.2-P4	n/a
TPS	2.9.1-p2	2.9.1-p2-sp27	n/a
TPS	3.0.tps-p2	3.0.tps-p2-sp6	n/a
HVA	2.7.2-P2		n/a
aGalaxy	2.5.2-P2		n/a

Mitigation Recommendations

Work-Around:

Disable SSL v3 on VIPs

Example:

In order to disable SSL v3 on the data plane for a particular connection, you need the following:

```
1.  Disable SSLV3 in the client-ssl template (cs in this example)
       A10(config)#slb template client-ssl cs
       A10(config-client ssl)# disable-sslv3

2.  Bind client-ssl template to SSL vport for a virtual-server (vip1 in this example)
       A10(config)#slb virtual-server vip1
       AX10(config-slb vserver)# port 443 https
       AX10(config-slb vserver-vport)# template client-ssl  cs
```

Using aFleX

For customers who would like to redirect clients to a page explaining how to upgrade, A10 provides an aFleX script that can be applied to HTTP and HTTPS Virtual Ports. A10 does recommend evaluation of the script for possible performance impacts if the specific platform currently has high CPU loads. In a lab environment, A10 has measured about 5-10% performance impact due to enabling of aFleX. If aFleX is enabled for other ruleset, no impact was observed. This script may be updated periodically if new information is gathered about this threat.

aFleX rule to redirect all SSL v3 clients to an upgrade page

Aflex: redirectscript1

```
when CLIENT_ACCEPTED {
TCP::collect
set red 0
}

when CLIENT_DATA {
binary scan [TCP::payload] cSSccSS rtype dumver rlen dum1 dum2 dum3 sslver
log $sslver
#   SSL 3.0 -> 768 TLS 1.0 -> 769 TLS 1.1 -> 770  TLS 1.2 -> 771
if { $sslver == 768 } { set red 1 }
}

when HTTP_REQUEST {
if {$red  == 1} {
  HTTP::respond 302 Location "http://example.com/upgradeyourbrowser.html" Cache-Control No-Cache Pragma No-Cache
}
}
```

How to configure aFleX on the virtual-server:

```
slb virtual-server vip1 X.X.X.X
   port 443  https
      source-nat pool pool
      service-group sg2
      template client-ssl template1
      aflex redirectscript1
```

In addition to that, A10 provides an aFleX script that would allow the customer of 2.6.1 and 2.7.0 to drop connection since the **sslv3 disable** command is not available.

aFleX rules for dropping all SSL v3 requests

Aflex: dropscript1

```
when CLIENT_ACCEPTED {
TCP::collect
}

when CLIENT_DATA {
binary scan [TCP::payload] cSSccSS rtype dumver rlen dum1 dum2 dum3 sslver
log "sslver $sslver"
#   SSL 3.0 -> 768 TLS 1.0 -> 769 TLS 1.1 -> 770  TLS 1.2 -> 771
if { $sslver == 768 } { reject }
}
```

How to configure aFleX on the virtual-server:

```
slb virtual-server vip1 X.X.X.X
   port 443  https
      source-nat pool pool
      service-group sg2
      template client-ssl template1
      aflex dropscript1
```