Netgear Signed TLS Cert Private Key Disclosure

Nicholas Starke | https://twitter.com/nstarke | https://github.com/nstarke

Overview

There are at least two valid, signed TLS certificates that are bundled with publicly available Netgear device firmware.

These certificates are trusted by browsers on all platforms, but will surely be added to revocation lists shortly.

The firmware images that contained these certificates along with their private keys were publicly available for download through Netgear's support website, without authentication; thus anyone in the world could have retrieved these keys.

routerlogin.net

Both keys found were contained in the `R9000-V1.0.5.8` firmware image file available here: `http://www.downloads.netgear.com/files/GDC/R9000/R9000-V1.0.5.8.zip`

This is the output from reading the certificate file in openssl:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            c1:a1:00:64:07:61:2c:07:00:00:00:00:50:f1:09:6a
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, O = "Entrust, Inc.", OU = See
www.entrust.net/legal-terms, OU = "(c) 2012 Entrust, Inc. - for authorized
use only", CN = Entrust Certification Authority - L1K
        Validity
            Not Before: May  1 00:23:51 2019 GMT
            Not After : Jul 30 00:53:50 2021 GMT
        Subject: C = US, ST = California, L = San Jose, O = "Netgear, Inc",
CN = www.routerlogin.net
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:c9:6d:0a:79:c9:ca:64:cd:ea:f0:ac:f4:bf:f6:
                    37:2b:1b:5a:f9:2c:10:52:d6:ee:4e:21:d3:00:2b:
                    18:fd:08:a0:6b:92:26:86:40:26:ef:f3:b7:dc:4d:
                    63:b8:04:0e:a0:78:bc:87:4e:50:d6:2d:3c:d4:f1:
                    ed:b8:10:9c:bf:e7:eb:59:a9:19:4d:f7:dc:73:9d:
                    b0:13:0a:29:41:4e:47:25:25:11:18:64:83:67:bd:
                    77:6d:22:b3:1f:df:db:29:09:20:d9:a1:3f:67:95:
                    83:ce:7e:02:c8:6f:46:46:f5:60:1b:75:30:8a:dc:
                    c4:a0:e6:e3:97:e0:f5:d7:ce:15:21:2d:26:c2:ef:
                    66:a6:79:bf:ac:28:af:e2:d4:7f:6e:8d:31:a5:07:
```

```
                    fa:c6:e2:91:cc:b0:cf:c8:27:4c:f1:8d:d8:14:8b:
                    ca:d5:c7:2b:10:72:12:66:63:46:02:1b:f2:ab:8a:
                    a2:1c:18:39:1f:4c:ed:a9:ca:ed:e7:05:96:a6:6a:
                    a0:ab:76:bd:68:c6:ee:43:4d:e4:51:ce:79:a3:0b:
                    81:7c:ea:67:87:75:03:25:ee:5f:f9:67:d7:12:a8:
                    76:c5:a3:37:35:5f:d1:61:26:ab:9a:f3:b3:7d:4d:
                    d1:24:73:ed:d7:74:3e:e8:b9:d5:4e:d7:9f:b5:f2:
                    46:c5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                DNS:www.routerlogin.net, DNS:routerlogin.net,
DNS:www.routerlogin.com, DNS:routerlogin.com
            CT Precertificate SCTs:
                Signed Certificate Timestamp:
                    Version   : v1 (0x0)
                    Log ID    :
55:81:D4:C2:16:90:36:01:4A:EA:0B:9B:57:3C:53:F0:

C0:E4:38:78:70:25:08:17:2F:A3:AA:1D:07:13:D3:0C
                    Timestamp : May  1 00:53:53.294 2019 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256

30:44:02:20:0B:F3:9B:CB:60:8F:CE:00:51:E5:BE:2A:

61:21:2D:F6:4A:4F:AE:A8:B6:86:6D:D4:3F:30:1B:93:

42:C5:F5:B0:02:20:24:62:CD:72:37:EF:B9:D9:25:DF:

28:BC:56:E3:79:B2:21:14:58:2B:4B:05:78:D2:69:66:
                                8E:89:1A:65:32:4C
                Signed Certificate Timestamp:
                    Version   : v1 (0x0)
                    Log ID    :
87:75:BF:E7:59:7C:F8:8C:43:99:5F:BD:F3:6E:FF:56:

8D:47:56:36:FF:4A:B5:60:C1:B4:EA:FF:5E:A0:83:0F
                    Timestamp : May  1 00:53:53.333 2019 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256

30:44:02:20:16:80:A7:86:0B:EA:DD:3F:0A:6B:5D:10:

1E:C3:E2:8A:92:F7:6F:28:85:9D:64:FA:CF:24:F8:02:

C5:A5:15:0C:02:20:34:D0:90:D7:4C:6D:14:56:49:5C:

DC:A6:B1:18:BC:29:32:F0:37:0A:B7:A9:5F:43:37:DC:
                                B2:F2:A4:FA:FA:AA
                Signed Certificate Timestamp:
                    Version   : v1 (0x0)
                    Log ID    :
56:14:06:9A:2F:D7:C2:EC:D3:F5:E1:BD:44:B2:3E:C7:
```

```
46:76:B9:BC:99:11:5C:C0:EF:94:98:55:D6:89:D0:DD
                    Timestamp : May  1 00:53:53.346 2019 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256

30:45:02:21:00:86:C3:D7:ED:C6:80:41:33:FC:6F:8F:

36:00:67:BB:58:F4:52:85:D7:1F:EF:46:E5:E1:1C:1F:

55:40:75:EC:DB:02:20:4B:2A:41:34:4D:5E:FD:FA:87:

C5:E8:A1:26:9C:EF:DE:BA:09:7A:24:6D:8E:2A:46:6F:
                                12:EB:4B:DE:A4:5E:62
                Signed Certificate Timestamp:
                    Version   : v1 (0x0)
                    Log ID    :
F6:5C:94:2F:D1:77:30:22:14:54:18:08:30:94:56:8E:

E3:4D:13:19:33:BF:DF:0C:2F:20:0B:CC:4E:F1:64:E3
                    Timestamp : May  1 00:53:53.335 2019 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256

30:45:02:21:00:E9:65:92:90:57:A3:FC:D6:5C:B1:32:

1B:F9:AF:78:85:91:F8:72:43:95:98:38:33:E6:75:A4:

FC:AA:29:BF:15:02:20:79:8A:8A:8F:44:F2:72:E5:05:

5F:7D:5E:FA:95:41:03:AA:BE:BF:95:44:5C:12:A5:C8:
                                6D:EE:31:E3:D6:E3:1F
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client
Authentication
            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://crl.entrust.net/level1k.crl

            X509v3 Certificate Policies:
                Policy: 2.16.840.1.114028.10.1.5
                  CPS: http://www.entrust.net/rpa
                Policy: 2.23.140.1.2.2

            Authority Information Access:
                OCSP - URI:http://ocsp.entrust.net
                CA Issuers - URI:http://aia.entrust.net/l1k-chain256.cer

            X509v3 Authority Key Identifier:

keyid:82:A2:70:74:DD:BC:53:3F:CF:7B:D4:F7:CD:7F:A7:60:C6:0A:4C:BF
```

```
            X509v3 Subject Key Identifier:
                5D:17:F2:BC:F7:B8:2D:0B:B8:4C:E8:EA:A2:79:E9:10:65:29:62:9D
            X509v3 Basic Constraints:
                CA:FALSE
    Signature Algorithm: sha256WithRSAEncryption
         21:36:ac:a8:3a:e8:47:17:90:dd:d8:5c:e0:27:78:f1:d6:f9:
         b8:94:29:64:76:8f:79:4c:51:7b:c6:2c:e7:78:4f:6c:c3:3c:
         18:55:3e:48:ba:0d:65:2f:5c:0c:7a:8c:8b:cd:7e:d9:fc:e3:
         89:54:07:41:2c:e9:f6:7f:bc:eb:22:e0:45:20:5c:5b:1d:87:
         9c:19:38:76:fd:65:67:57:43:8e:eb:5d:1d:4e:81:bd:7e:53:
         0a:7b:85:aa:13:ba:7e:bc:eb:87:2d:51:44:3e:5b:54:71:82:
         b0:a4:69:4a:7d:f9:ea:df:51:f2:f8:53:a8:5c:6e:34:71:8c:
         1d:d5:16:57:cc:80:37:4d:2c:8d:5c:79:2d:4e:22:d0:ef:42:
         ea:f9:21:4f:e9:b2:95:1a:4d:cc:0c:e2:87:2c:a4:1a:ed:a0:
         55:0f:52:0c:24:b3:dc:1e:fd:f8:cf:df:91:3c:98:a7:8f:9f:
         e6:da:92:f7:13:d4:91:c2:cb:0a:40:12:fa:a0:db:57:4c:30:
         ae:65:47:5a:25:a5:40:7c:98:1e:2d:51:40:82:cc:5d:5c:34:
         d1:01:8d:e3:29:55:b1:f5:59:59:7c:55:72:e2:59:99:87:64:
         3d:2b:9f:56:e9:53:13:73:af:ab:4c:e1:d8:26:be:73:7c:78:
         d7:0a:12:42
```

According to the above output, this certificate, which is signed by EnTrust, is valid for the following DNS host names:

- www.routerlogin.net
- routerlogin.net
- www.routerlogin.com
- routerlogin.com

The corresponding private key for this certificate is:

```
-----BEGIN PRIVATE KEY-----
MIIEvwIBADANBgkqhkiG9w0BAQEFAASCBKkwggSlAgEAAoIBAQDJbQp5ycpkzerw
rPS/9jcrG1r5LBBS1u5OIdMAKxj9CKBrkiaGQCbv87fcTWO4BA6geLyHTlDWLTzU
8e24EJy/5+tZqRlN99xznbATCilBTkclJREYZINnvXdtIrMf39spCSDZoT9nlYPO
fgLIb0ZG9WAbdTCK3MSg5uOX4PXXzhUhLSbC72ameb+sKK/i1H9ujTGlB/rG4pHM
sM/IJ0zxjdgUi8rVxysQchJmY0YCG/KriqIcGDkfTO2pyu3nBZamaqCrdr1oxu5D
TeRRznmjC4F86meHdQMl7l/5Z9cSqHbFozc1X9FhJqua87N9TdEkc+3XdD7oudVO
15+18kbFAgMBAAECggEAXO3t01qCAhfuuLNTB+10bnLkeekWbuGyeGGqk31Ovg7o
1DhNhcq7LCFpRj5+LzvP88FAWbyMFwQv+J7VagJgDznUnz0g65PbJYwu29noRrTy
pfR/+p0E8yu6maNUuPPyjPAlM8LtGcElWnNQnWCZL8utV32ts6M/JGzhvASR58ne
5M6fB3RPgfoe50zaBu7lQ5YhlNpj8J0P1eg0gl/535nx2FqejqqkBu10xfo3T3dA
KdJIuNA3rU9BHjzYl/+8SKZ9wYekuf79CM+zSrVe2iJ7gZP2V3XhUdtKgL8ZgNHG
TNW4LOIOvG7/4XH+GkacspjC5ZA/OOlx/yqXzkE/UQKBgQDoyRhy5jBF0TNPrR1A
smQK+t1eEI27LbM7cFnldlbGa/gP+3U8zPMBGru7fdED9dVzJ+2p6lzHkDAP3KcT
ftOIeABWtGWZ724whxDu996BeXI0lnWjY8dEUT3aod9lpC/PUiCV+MmUSTPBFXMl
bF5ZA+dpbmp7IBP/7FIdRveuPwKBgQDdg1mW2sm0GdeEETu3oeK4Xi+7X63jhc33
VsBJ5285RmQWLPbMAANirHIQ+mTU4XIn24LNfugteT5ocJlY7TjTje4ldNY5k0Ha
9tJYMD3ZnmT++NEFM919vaelCoGMj0K2KUYZ4ef/IT9iisUA+Wz9HL5So99J/RFw
```

```
Hhr5D+fR+wKBgQCVAGsq2Jabid27KUbpK4aH1K2vUQ83eXgZGsAf9VBz75Y3vK/9
O/5rfY4e49jPHSMEc9FXipDamDt7W7SB8RM7bfxhg1TpZG12mG3JWFVPMMpeSNSB
whNBcnMSJ7zT1XVY0evTswxsYzLCa5VppeT6O1p7jNaReyXyEXU6EjvlhwKBgQCW
rBuqUxPUH6fKu3YlSEZRJi/Ngh1jn8YjsayGGJg9GzZFJzyQMooa+jV0ev1PGDJw
Dg4A/YusMsZSgBSuul1m+Sm97KUy8IlhCXa2acoIVodYL6LtqQPF3dVEm8rW8zNr
eNOoE1Oc5N6ahs3OBdsup/iFedYOG8davf+W3kzPNQKBgQCVJ1ehlnFwT8bFs+PU
hgrLHrvh6XHqcdJ1NOR52Su5Ge0ZdaAFtisSoJm2bVpbfyFJbfjMRg1FdhZr71Kb
LLG0IuutcnTua/FicLhUjFT5qrfs9he8trAhMgjT4t4HCH0H19JoaEOUUU8FMPLi
QZbodRspSr2dBf316Kh1N8C8Yg==
-----END PRIVATE KEY-----
```

These files were found respectively at `/etc/uhttpd.crt` and `/etc/uphttpd.key` in the aforementioned firmware image.

mini-app.funjsq.com

In the same firmware image was an additional valid TLS Certificate and its corresponding private key.

The files were found at the paths `/data/funjsq/config/httpd/cert.pem` and `/data/funjsq/config/httpd/key.pem`.

The openssl output for this certificate is:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            bf:c0:c9:fd:2e:8c:92:ec:4e:bf:10:d8:c1:28:3d:0b
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = GB, ST = Greater Manchester, L = Salford, O = COMODO CA
Limited, CN = COMODO RSA Domain Validation Secure Server CA
        Validity
            Not Before: Jul 26 00:00:00 2018 GMT
            Not After : Jul 25 23:59:59 2020 GMT
        Subject: OU = Domain Control Validated, OU = PositiveSSL, CN =
mini-app.funjsq.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:cc:57:d5:45:ad:bd:60:c8:af:6f:50:97:ef:df:
                    67:b0:1d:69:1d:a3:75:e9:ba:08:8d:4c:54:2e:b6:
                    83:1c:2e:e1:1f:66:0c:fb:7a:d0:9a:ce:52:a4:3f:
                    75:70:f4:39:73:f3:f5:86:2e:96:59:e6:a5:54:62:
                    17:52:15:ad:6f:22:bd:7d:84:36:14:7a:3b:1c:60:
                    61:7a:7d:86:d8:e2:99:49:d4:06:e9:7a:00:f2:43:
                    f9:11:87:06:c8:20:0e:fc:15:51:bb:13:9d:ed:27:
                    39:df:cd:ec:46:6f:ed:a7:56:4f:71:a3:46:d7:25:
                    f2:5a:38:a9:23:a1:89:0e:6e:f1:3d:6b:04:05:0e:
                    8b:32:bc:f1:1c:0e:f8:6c:95:e2:cd:6c:38:1a:e6:
```

```
                    a6:3f:3b:22:41:f7:23:45:36:82:58:3c:a5:89:aa:
                    6e:16:e0:32:c2:38:a8:42:ba:de:ae:b4:03:f3:0b:
                    a4:9e:6b:a6:31:68:14:da:20:93:aa:a7:a7:49:f4:
                    6d:3e:c8:39:72:e1:62:35:cc:67:3f:08:2e:ae:8b:
                    ac:fc:14:3b:9d:b8:c7:5b:9b:db:08:3a:2b:98:aa:
                    0e:3e:92:5c:e7:e6:db:13:bb:47:e0:3b:3d:60:e5:
                    f3:22:e8:8f:01:04:cf:e3:c3:fc:7e:e2:6c:23:2c:
                    48:17
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:

keyid:90:AF:6A:3A:94:5A:0B:D8:90:EA:12:56:73:DF:43:B4:3A:28:DA:E7

            X509v3 Subject Key Identifier:
                27:B5:A2:32:E3:84:92:C6:D3:38:A3:83:6A:61:B2:C0:E7:43:53:1D
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client
Authentication
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.6449.1.2.2.7
                  CPS: https://secure.comodo.com/CPS
                Policy: 2.23.140.1.2.1

            X509v3 CRL Distribution Points:

                Full Name:

URI:http://crl.comodoca.com/COMODORSADomainValidationSecureServerCA.crl

            Authority Information Access:
                CA Issuers -
URI:http://crt.comodoca.com/COMODORSADomainValidationSecureServerCA.crt
                OCSP - URI:http://ocsp.comodoca.com

            X509v3 Subject Alternative Name:
                DNS:mini-app.funjsq.com, DNS:www.mini-app.funjsq.com
            CT Precertificate SCTs:
                Signed Certificate Timestamp:
                    Version   : v1 (0x0)
                    Log ID    :
EE:4B:BD:B7:75:CE:60:BA:E1:42:69:1F:AB:E1:9E:66:

A3:0F:7E:5F:B0:72:D8:83:00:C4:7B:89:7A:A8:FD:CB
                    Timestamp : Jul 26 14:44:17.854 2018 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256

30:46:02:21:00:94:5A:FE:A8:70:93:59:E5:0A:F1:B5:
```

```
29:FE:2E:0D:91:34:D5:A8:A9:1D:C1:63:77:16:F3:75:

67:16:6C:25:33:02:21:00:93:66:BA:D6:27:57:D8:59:

A5:C7:73:87:23:AB:F9:84:D9:DD:BA:50:A7:FC:5E:8E:
                                40:74:A0:DD:9C:BA:CF:BD
                Signed Certificate Timestamp:
                    Version   : v1 (0x0)
                    Log ID    :
5E:A7:73:F9:DF:56:C0:E7:B5:36:48:7D:D0:49:E0:32:

7A:91:9A:0C:84:A1:12:12:84:18:75:96:81:71:45:58
                    Timestamp : Jul 26 14:44:18.391 2018 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256

30:45:02:21:00:F1:07:91:63:03:B7:51:60:5F:ED:FD:

72:43:E7:8F:98:34:A8:9E:85:CF:C1:33:AB:AF:7C:C1:

B3:16:75:A8:79:02:20:30:F7:DB:8E:C7:D3:9F:86:42:

80:B7:C6:6B:0D:D5:14:85:99:BC:3F:99:79:D3:43:24:
                                3C:17:4F:2E:BE:A6:6A
                Signed Certificate Timestamp:
                    Version   : v1 (0x0)
                    Log ID    :
55:81:D4:C2:16:90:36:01:4A:EA:0B:9B:57:3C:53:F0:

C0:E4:38:78:70:25:08:17:2F:A3:AA:1D:07:13:D3:0C
                    Timestamp : Jul 26 14:44:17.893 2018 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256

30:45:02:21:00:F8:DF:94:32:61:C5:71:5F:D5:84:87:

15:58:57:B8:9E:9F:81:88:A5:3A:4E:C1:8A:6E:73:38:

19:FD:33:9B:D4:02:20:73:80:2E:EE:4F:1D:F0:08:9A:

1D:85:FB:51:D8:66:7A:96:2F:C0:12:4E:EF:AD:2E:1D:
                                6E:B7:FC:3D:7D:DB:B8
    Signature Algorithm: sha256WithRSAEncryption
         61:da:c4:80:ee:eb:f7:67:95:31:b8:55:7f:27:64:30:68:9f:
         5e:2d:5c:40:cc:a7:12:f9:74:a6:e8:b1:d2:10:b7:c8:99:80:
         05:25:56:d1:51:59:5d:54:d9:a5:bd:c5:d4:ac:da:16:73:d9:
         8d:97:cc:f5:64:85:3d:1f:02:c4:37:b5:7b:9a:06:fb:a0:bf:
         d4:27:11:c0:98:f0:28:aa:84:bc:3b:bf:67:18:cc:3d:13:46:
         4d:18:9b:ca:62:09:52:2d:df:df:b2:4b:ac:fb:b2:7d:58:16:
         39:87:20:d6:c9:82:cf:e5:2a:9d:e9:6d:7f:6f:56:6d:b7:a4:
         be:54:c4:ed:4a:73:74:10:b4:a2:94:e9:10:4a:69:9d:60:0d:
         ec:45:4c:e4:12:d9:ab:ce:28:fc:da:4e:e7:d6:90:3e:87:2b:
         2d:24:de:79:84:10:95:c7:be:4a:9f:c7:b2:64:0e:b3:0d:3e:
         15:7c:32:c4:84:3a:d7:b5:67:96:0e:cc:3c:5e:e3:a0:cb:31:
```

```
         d0:81:85:af:1e:bc:a6:fd:84:ec:76:e9:31:95:6a:dc:de:49:
         59:24:14:66:a7:69:6b:f0:4d:14:1f:e2:31:f9:42:1d:d8:76:
         9f:08:0a:2b:5c:53:8f:86:60:5a:65:ce:6a:dc:56:ef:b7:30:
         69:f3:37:ec
-----BEGIN CERTIFICATE-----
MIIG4TCCBcmgAwIBAgIRAL/Ayf0ujJLsTr8Q2MEoPQswDQYJKoZIhvcNAQELBQAw
gZAxCzAJBgNVBAYTAkdCMRswGQYDVQQIExJHcmVhdGVyIE1hbmNoZXN0ZXIxEDAO
BgNVBAcTB1NhbGZvcmQxGjAYBgNVBAoTEUNPTU9ETyBDQSBMaW1pdGVkMTYwNAYD
VQQDEy1DT01PRE8gUlNBIERvbWFpbiBWYWxpZGF0aW9uIFNlY3VyZSBTZXJ2ZXIg
Q0EwHhcNMTgwNzI2MDAwMDAwWhcNMjAwNzI1MjM1OTU5WjBXMSEwHwYDVQQLExhE
b21haW4gQ29udHJvbCBWYWxpZGF0ZWQxFDASBgNVBAsTC1Bvc2l0aXZlU1NMMRww
GgYDVQQDExNtaW5pLWFwcC5mdW5qc3EuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAzFfVRa29YMivb1CX799nsB1pHaN16boIjUxULraDHC7hH2YM
+3rQms5SpD91cPQ5c/P1hi6WWealVGIXUhWtbyK9fYQ2FHo7HGBhen2G2OKZSdQG
6XoA8kP5EYcGyCAO/BVRuxOd7Sc5383sRm/tp1ZPcaNG1yXyWjipI6GJDm7xPWsE
BQ6LMrzxHA74bJXizWw4GuamPzsiQfcjRTaCWDyliapuFuAywjioQrrerrQD8wuk
nmumMWgU2iCTqqenSfRtPsg5cuFiNcxnPwgurous/BQ7nbjHW5vbCDormKoOPpJc
5+bbE7tH4Ds9YOXzIuiPAQTP48P8fuJsIyxIFwIDAQABo4IDbDCCA2gwHwYDVR0j
BBgwFoAUkK9qOpRaC9iQ6hJWc99DtDoo2ucwHQYDVR0OBBYEFCe1ojLjhJLG0zij
g2phssDnQ1MdMA4GA1UdDwEB/wQEAwIFoDAMBgNVHRMBAf8EAjAAMB0GA1UdJQQW
MBQGCCsGAQUFBwMBBggrBgEFBQcDAjBPBgNVHSAESDBGMDoGCysGAQQBsjEBAgIH
MCswKQYIKwYBBQUHAgEWHWh0dHBzOi8vc2VjdXJlLmNvbW9kby5jb20vQ1BTMAgG
BmeBDAECATBUBgNVHR8ETTBLMEmgR6BFhkNodHRwOi8vY3JsLmNvbW9kb2NhLmNv
bS9DT01PRE9SU0FEb21haW5WYWxpZGF0aW9uU2VjdXJlU2VydmVyQ0EuY3JsMIGF
BggrBgEFBQcBAQR5MHcwTwYIKwYBBQUHMAKGQ2h0dHA6Ly9jcnQuY29tb2RvY2Eu
Y29tL0NPTU9ET1JTQURvbWFpblZhbGlkYXRpb25TZWN1cmVTZXJ2ZXJDQS5jcnQw
JAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLmNvbW9kb2NhLmNvbTA3BgNVHREEMDAu
ghNtaW5pLWFwcC5mdW5qc3EuY29tghd3d3cubWluaS1hcHAuZnVuanNxLmNvbTCC
AX8GCisGAQQB1nkCBAIEggFvBIIBawFpAHcA7ku9t3XOYLrhQmkfq+GeZqMPfl+w
ctiDAMR7iXqo/csAAAFk1wwxPgAABAMASDBGAiEAlFr+qHCTWeUK8bUp/i4NkTTV
qKkdwWN3FvN1ZxZsJTMCIQCTZrrWJ1fYWaXHc4cjq/mE2d26UKf8Xo5AdKDdnLrP
vQB2AF6nc/nfVsDntTZIfdBJ4DJ6kZoMhKESEoQYdZaBcUVYAAABZNcMM1cAAAQD
AEcwRQIhAPEHkWMDt1FgX+39ckPnj5g0qJ6Fz8Ezq698wbMWdah5AiAw99uOx9Of
hkKAt8ZrDdUUhZm8P5l500MkPBdPLr6magB2AFWB1MIWkDYBSuoLm1c8U/DA5Dh4
cCUIFy+jqh0HE9MMAAABZNcMMWUAAAQDAEcwRQIhAPjflDJhxXFf1YSHFVhXuJ6f
gYilOk7Bim5zOBn9M5vUAiBzgC7uTx3wCJodhftR2GZ6li/AEk7vrS4dbrf8PX3b
uDANBgkqhkiG9w0BAQsFAAOCAQEAYdrEgO7r92eVMbhVfydkMGifXi1cQMynEvl0
puix0hC3yJmABSVW0VFZXVTZpb3F1KzaFnPZjZfM9WSFPR8CxDe1e5oG+6C/1CcR
wJjwKKqEvDu/ZxjMPRNGTRibymIJUi3f37JLrPuyfVgWOYcg1smCz+Uqneltf29W
bbekvlTE7UpzdBC0opTpEEppnWAN7EVM5BLZq84o/NpO59aQPocrLSTeeYQQlce+
Sp/HsmQOsw0+FXwyxIQ617Vnlg7MPF7joMsx0IGFrx68pv2E7HbpMZVq3N5JWSQU
Zqdpa/BNFB/iMflCHdh2nwgKK1xTj4ZgWmXOatxW77cwafM37A==
-----END CERTIFICATE-----
```

The corresponding private key is:

```
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDMV9VFrb1gyK9v
UJfv32ewHWkdo3XpugiNTFQutoMcLuEfZgz7etCazlKkP3Vw9Dlz8/WGLpZZ5qVU
YhdSFa1vIr19hDYUejscYGF6fYbY4plJ1AbpegDyQ/kRhwbIIA78FVG7E53tJznf
zexGb+2nVk9xo0bXJfJaOKkjoYkObvE9awQFDosyvPEcDvhsleLNbDga5qY/OyJB
9yNFNoJYPKWJqm4W4DLCOKhCut6utAPzC6Sea6YxaBTaIJOqp6dJ9G0+yDly4WI1
```

```
zGc/CC6ui6z8FDuduMdbm9sIOiuYqg4+klzn5tsTu0fgOz1g5fMi6I8BBM/jw/x+
4mwjLEgXAgMBAAECggEANCH0d2Jr/lU07OFS4g/NFFFsj/M0Ef00UVg34fMOYBJV
vPz8MuySa+xXiS/ndnnYboy/Bwy7rxP4+h5MdNSy+reSQIOKiI7mpcaxF98OmCa3
lO5TFR3bP/O3h5E7WbNUH1wRDfljQS3QxhhzP0UvDJIokoVlfV5hBkOOY1jC7rtK
KtdInqD0y+ALkxDAj5yk/8kSxSirO5/3nzZAgzQxGr2r2psytEQlVMqRD4rcLymH
WQ2GeZe0gr9wcWiFDvFBc3S7Blh476BdNKbNuvplYdHq1PKnD1b2NegBIzYH+fb6
DE+XLCrSADwDbIE//L4B+fvK6eOciMPqvmUD2mPGAQKBgQD2Qcu7LexNlKbk3B8v
BBYwSda+GCclvnAAZdBrEtp++nuCHhusk6UokM4e3Xabq8//pFm9UDaGdmW0S+Bs
37TvcbWNidpJ7hEOS93sQ9dp/08GQKRb/tAfHRJ/GRgnd9tJKvuQwx/5PRBl4gJb
EROFG+zNnNSFXZU8i0pwxUig0QKBgQDUbYOMm7Py8sYSU5dLfCPCvLFdYCddppfh
7wwFduF1ipqTfhFejOy+2TnxHFOEBX96GfNRwtgP5FmKMEmbSYELEH7V+6yJus+k
MGxck6+pD2aX7bIUA96HOHCCOUA4zE6V/aN7nIon+jgtj2vkjB3m7FCv6Tu05jTS
C1wsXv9UZwKBgQDs2SGTGTsy7uuKKPDRLpQMw6gH04ErezuMFmDb6xk9kbrizgR9
+s+Z8ZRd+VFPrnNyhGdPfuvCbfOp8mSbMpp6xhoBVPofqxq6blu3FxUDvOwLrnam
iLExi6uzlLY3l77QY8frVtDUzleMNlFft0/X8aDTrah10SltPudNCWKuUQKBgEy2
e8IkXHjI6XSm0UVGQFfL8rVIyw6L4d+KhynWA5eCBU5sQXOGqtxE8CK9Wv+bSKzc
gD0vgv1CNn+r7njws3Q+cb9u0qEuYFvnzMol31LLJ/6HrT6DIzJr1F2CtUmNpneO
ECLMpivHtc/mMk1nuEizYHQWYyRx2fNcfN3dNJHTAoGBALeEHU0qn883Us/iyftC
mB4CqgWDJ22jhDWbpu/mdagCymRWuP8hPHXlGcMSBSo2fZz9TBx9p5dAJkXSbUd+
BiG73boMCjmNrJnB+06rh7lwcPIGpD3XAhQ14rm7YUC8Y7VAUGw6e/H51zOJ+eQx
xqGaW9IOaJ7fMqT2LMo1yENb
-----END PRIVATE KEY-----
```

The DNS host name for the certificate is `mini-app.funjsq.com`.

Rationale for Full Disclosure

We are aware that Netgear has public bug bounty programs. However, at current date those programs do not allow public disclosure under any circumstances.

We as researchers felt that the public should know about these certificate leaks in order to adequately protect themselves and that the certificates in question should be revoked so that major browsers do not trust them any longer. We could not guarantee either if we had used the existing bug bounty programs.

Disclosure Timeline

- Tuesday, January 14th 2020 - Initial Discovery
- Tuesday, January 14 2020 - Tweet sent attempting to establish communications with Netgear
- Wednesday, January 15 2020 - Reached out to Bugcrowd to attempt to establish communications.
- Thursday, January 16 - Bugcrowd responds, but we are unable to establish a communications channel outside of the Netgear bug bounty programs.
- Friday, Jaunary 17th - Conversation with bugcrowd proves inconclusive
- Sunday, January 19th - Feeling we have exhausted our disclosure avenues, we decide to publish

Credits

- Tom Pohl (@tompohl)
- Nick Starke (@nstarke)