Vulnerability Details

Product Overview

Citrix Online is a web-based remote access and collaboration software[1] widely used in many corporations. Multiple Citrix products are mainly based on this technology (GoToMeeting[3], GoToMyPc[2], GoToTraining[5], GoToWebinar[4], GoToAssist [6]) as it allows to easily share and interact with users' desktops.

"*GoToMeeting users can collaborate on documents, deliver presentations, perform product demonstrations and securely share confidential information from anywhere, at any time. GoToMeetings rapid download, quick meeting setup and intuitive user interface has meeting organizers and attendees up and running in a matter of seconds.*"

As mentioned in the product's documentation[7], the quick application installation and setup is managed via a Java applet. This component is signed with a valid certificate issued by VeriSign to Citrix Online.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            0c:41:d5:a0:df:13:0d:d5:cf:17:2d:a0:0d:e8:fa:5a
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network,
        OU=Terms of use at https://www.verisign.com/rpa (c)04,
        CN=VeriSign Class 3 Code Signing 2004 CA
        Validity
            Not Before: May  6 00:00:00 2009 GMT
            Not After : Jun 30 23:59:59 2012 GMT
        Subject: C=US, ST=Florida, L=Fort Lauderdale, O=Citrix Online,
        OU=Digital ID Class 3 - Java Object Signing,
        OU=Online, CN=Citrix Online
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:90:f6:a6:c4:ae:7a:be:eb:ca:9f:1c:f4:6d:85:
                    d8:c5:ce:c9:8b:eb:3a:64:d5:64:4f:e6:cf:06:2f:
                    e0:a3:4b:b1:3f:62:6f:9e:71:de:4f:92:9c:90:25:
                    32:59:8a:15:49:51:a9:86:f4:cc:ad:67:1e:3a:25:
                    8a:81:77:7b:36:1b:17:9d:b5:53:15:75:c0:98:12:
                    80:8b:60:79:c4:f9:d5:cc:af:b5:15:02:a6:c1:97:
                    82:6f:b5:38:b8:df:19:d5:af:6f:3c:41:66:a6:2e:
                    07:87:5c:e6:bb:9e:77:60:55:f6:5a:7d:4d:29:53:
                    82:fe:b4:5f:b4:65:72:26:23
                Exponent: 65537 (0x10001)
        X509v3 extensions:
```

```
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Key Usage: critical
                Digital Signature
            X509v3 CRL Distribution Points:
                URI:http://CSC3-2004-crl.verisign.com/CSC3-2004.crl

            X509v3 Certificate Policies:
                Policy: 2.16.840.1.113733.1.7.23.3
                  CPS: https://www.verisign.com/rpa

            X509v3 Extended Key Usage:
                Code Signing
            Authority Information Access:
                OCSP - URI:http://ocsp.verisign.com
                CA Issuers - URI:http://CSC3-2004-aia.verisign.com/CSC3-2004-aia.cer

            X509v3 Authority Key Identifier:
                keyid:08:F5:51:E8:FB:FE:3D:3D:64:36:7C:68:CF:5B:78:A8:DF:B9:C5:37

            Netscape Cert Type:
                Object Signing
            1.3.6.1.4.1.311.2.1.27:
                0.......
    Signature Algorithm: sha1WithRSAEncryption
        4a:92:f4:8d:df:54:d2:43:93:7b:2e:1b:db:99:fe:86:ce:d9:
        91:14:02:3f:de:05:48:90:ab:51:4d:8a:71:15:6f:1c:61:8d:
        f8:47:33:d9:48:b0:a1:b0:b3:a2:a0:1e:49:a7:4a:35:d2:7b:
        17:1a:28:5e:27:e5:36:4a:06:81:94:a8:b0:38:0f:8f:6d:32:
        df:c4:63:3e:04:63:1e:c7:0c:4d:06:35:3c:9b:7d:ff:d9:d1:
        01:2c:87:63:9a:f0:df:5b:d7:af:49:73:0d:e7:12:0d:62:af:
        fe:bb:71:0c:37:53:ee:c3:b9:97:6d:95:ee:40:f5:bf:f0:df:
        22:95:26:49:90:79:13:da:56:7a:3b:7f:ee:07:c0:8d:00:22:
        2f:70:69:0b:2e:08:f7:d7:46:bb:fb:6d:96:42:b4:7b:08:ab:
        c3:16:f0:a3:94:27:3f:f0:89:8e:dd:b1:53:e1:eb:8e:02:a3:
        7c:99:5c:dc:e9:26:c5:08:38:60:ef:e0:20:6d:b0:e8:ff:34:
        12:1e:ab:e2:b0:4f:25:02:3d:dc:64:e7:2f:82:32:71:82:36:
        90:d0:f4:3b:93:d3:e6:72:67:ae:e0:59:d8:b3:41:88:5a:ec:
        7a:71:4e:07:01:37:43:ca:1c:a4:b6:86:3b:78:08:41:ce:9b:
        f0:17:9a:23
```

The Citrix Online signed applet, packaged in a JAR file named *StarterJDK_20091211.jar*, is responsible for downloading the required binaries, properly checking MD5 digests, and executing the installation setup.

All operations are managed by the class *com.ec.programstarter.ProgramStarter* which extends "Applet".

As illustrated in Figure 1, a pop-up window is shown whenever a user runs the applet for the first time. Being a properly signed applet with a valid certificate, the Java environment informs the user that "*the digital signature has been validated by a trusted source*".

The warning message is not even shown if:

- The user has already executed the Citrix Online applet on the specific workstation
- The user has already executed any applet issued by Citrix Online and the check "Always trust content from this published" has been selected. It should be noted that this is the default configuration

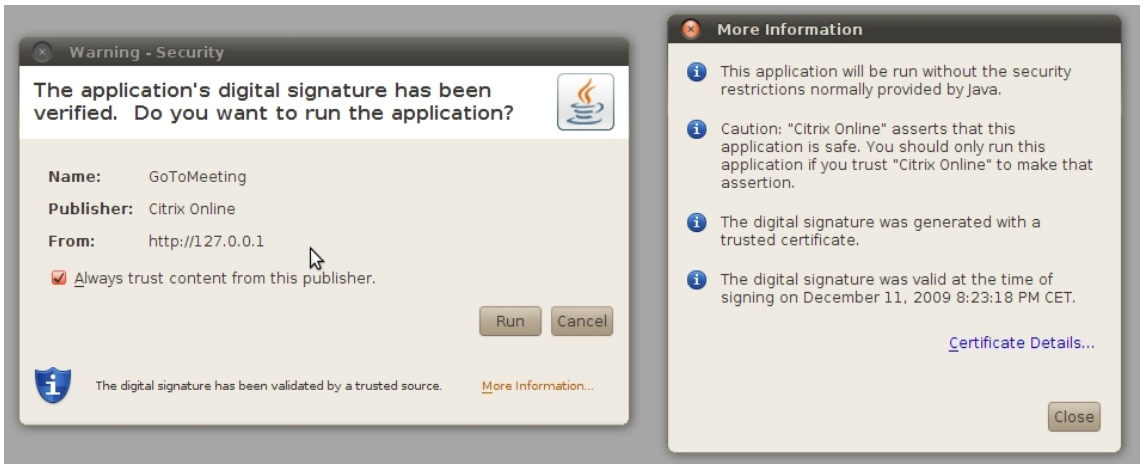

Figure 1: Citrix Online signed applet

Vulnerability Overview

An implementation flaw allows third parties to abuse secondary methods present in the signed applet in order to execute code on the victim's workstation. Successful exploitation leads to full system compromise under the credentials of the currently logged in user.

User interaction is required to exploit this vulnerability in that the target must visit a malicious page.

In detail, an attacker can abuse the "com.ec.programstarter.ProgramStarter.run()" method in order to execute arbitrary commands. Due to improper input validation, an attacker can easily tamper the "ProgramFile" and "ProgSize" parameters of the applet. However, a security control regarding the launching domain has been implemented by the developer in the applet *start()* method. This security check breaks the applet execution before that any operation takes actually place.

```
private static final String[] ALLOWED_DOMAINS = {
    "gotomypc.com",
    "gotoassist.com",
    "desktopstreaming.com",
    "fastsupport.com",
    "gotomeeting.com",
    "gototraining.com",
    "gotowebinar.com",
    "goview.com",
    "expertcity.com",
    "citrixonline.com" };

[...]

 public void start()
  {
    String str1 = super.getDocumentBase().getHost();
    int i = 0;
    for (int j = 0; j < ALLOWED_DOMAINS.length; ++j) {
      if ((str1.equals(ALLOWED_DOMAINS[j])) || (str1.endsWith("." + ALLOWED_DOMAINS[j]))) {
        i = 1;
        break;
      }
    }
    if (i == 0) {
```

```
this._infoLabel.setText("Error - Applet not hosted by one of our servers.");
debug("Applet not hosted by one of our servers, cannot trust it. host='" + str1 + "'");
ret
[...]
```

Abusing a secondary class ("com.ec.programstarter.GenericStarter"), an aggressor would still be able to properly initialize the applet's environment and execute a method containing a call to " Runtime.getRuntime().exec()" without dropping privileges. Executing Java methods via JavaScript allows us to bypass the Java mixed code checks (signed and unsigned Java instructions within the same context).

Workaround

Users need to manually tune the Java configuration in order to:

- Disable "Allow user to grant permissions to signed content"
- Enable "Check publisher certificate for revocation" and "Enable online certificate validation"

Please refer to [8] for a complete discussion on these problematics.

Bibliography

[1] Citrix Online Website, http://www.citrixonline.com/

[2] Citrix GoToMyPC https://www.gotomypc.com/

[3] Citrix GoToMeeting http://www.gotomeeting.com/fec/

[4] Citrix GoToWebinar http://www.gotomeeting.com/fec/webinar

[5] Citrix GoToTraining http://www.gotomeeting.com/fec/training/online_training

[6] Citrix GoToAssist http://www.gotoassist.com/

[7] GoToMeeting Presentation Server Administrators Installation Guide http://support.citrix.com/servlet/KbServlet/download/10875102-15208/CPS_Admin_Guide_for_G2M3.0.pdf

[8] Signed Java Applet Security: Worse than ActiveX? http://www.cert.org/blogs/vuls/2008/06/signed_java_security_worse_tha.html