

n.runs AG
 http://www.nruns.com/
 n.runs-SA-2011.001

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: Stack-Based Buffer Overflow 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 Citrix requests exploit code to reproduce issue
 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 stack-based buffer overflow 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.

The issue can be exploited with network access to the XML service interface. But exploitation can also be performed with unauthenticated access to the Citrix web frontend which is exposed to the Internet in many cases.

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.

The stack-based buffer overflow was identified in the wpnbr.dll extension DLL when parsing the <Password> element field. This element contains the obfuscated (CTX1 encoded) version of the password. If a plaintext password of more than 256 characters is provided this leads to the stack-based buffer overflow with the unicode version of the sent plaintext password in the current thread handler:

```
.text:64F6053D
.text:64F6053D 1oc_64F6053D:
.text:64F6053D
.text:64F6053D          push    ebx
.text:64F6053E          push    edi
.text:64F6053F          push    esi
.text:64F60540          lea    ecx, [ebp+dst_buffer_struct]
.text:64F60546          call   sub_64F6A910
.text:64F6054B          lea    ecx, [ebp+dst_buffer_struct]
.text:64F6054B          ; [ecx + 3c] points to the stack buffer
.text:64F6054B          ; which gets overflowed.
.text:64F60551          push   ecx
.text:64F60552          lea    ecx, [ebp+var_46B8]
.text:64F60558          mov    byte ptr [ebp+var_4], 18h
.text:64F6055C          ; The call to parse_received_msg() leads
.text:64F6055C          ; to the overflow of the local stack
.text:64F6055C          ; buffer in this function!
```


Credit:

Bug found and exploit developed by 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.