

[NT] Windows XP gethostbyaddr() NULL h_name Pointer

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-06/0071.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 06/22/03

To: list@securiteam.com

Date: 22 Jun 2003 19:53:12 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

Beyond Security in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at canadasales@beyondsecurity.com

Windows XP gethostbyaddr() NULL h_name Pointer

SUMMARY

It is possible to crash any application on Windows XP whenever `gethostbyaddr()` or `WSAAsyncGetHostByAddr()` function (from `ws2_32.dll`) are used for reverse name resolution (Mail and proxy servers, IRC clients, Peer-to-Peer clients, personal firewalls, etc). The crash occurs because a NULL pointer is returned as a reference instead of a valid entry.

DETAILS

Reproduction:

A test application can be downloaded from

<<http://www.security.nnov.ru/files/gethostbyaddr.zip>>

<http://www.security.nnov.ru/files/gethostbyaddr.zip>

1. Create zone `1.168.192.in-addr.arpa` and add record (Windows 2000 DNS server was used, results for `bind` may differ):

Securiteam: [NT] Windows XP gethostbyaddr() NULL h_name Pointer

254 IN CNAME non.existant.name

2. Use test program referenced

3. Tests on Windows NT 4.0, Windows 2000 and Windows XP SP1 resulted in:

Windows NT 4.0:

```
c:\>test.exe 192.168.1.254
gethostbyaddr failed
```

Windows 2000:

```
C:\>test.exe 192.168.1.254
gethostbyaddr failed
```

Windows XP SP1:

```
C:\>test.exe 192.168.1.254
h_name: (null)
```

We would expect that h_name never revert to a NULL value, if gethostbyaddr() returns a valid result.

ADDITIONAL INFORMATION

The information has been provided by <mailto:3APA3A@security.nnov.ru> 3APA3A. The vulnerability was first reported by at4r ins4n3. Further research was done by Roland Postle, Peter Pentchev and <mailto:3APA3A@security.nnov.ru> 3APA3A.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.