

[NT] Named Pipe Filename Local Privilege Escalation

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-07/0043.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 07/09/03

To: list@securiteam.com

Date: 9 Jul 2003 10:21:19 +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

Named Pipe Filename Local Privilege Escalation

SUMMARY

By specifying the name of a named pipe instead of a file, as an argument to SQL Server's xp_fileexist extended stored procedure, one can impersonate the user account Microsoft SQL Server is running under. This is due to the behavior of the CreateFile system call and Windows named pipe impersonation. This is not limited to Microsoft SQL Server, but a system wide-problem.

DETAILS

The API call CreateFile is used to open and/or create files, named pipes, mail slots and much more. Today, there is no mechanism in this API call to limit what kind of resource one wants to open. This is due to the fact that most resources are implemented as part of the file system.

Most services in WIN32 are running under the local system account and handling files in one way or another. If there exists a way to specify

Securiteam: [NT] Named Pipe Filename Local Privilege Escalation

which file a service should open, it is possible to impersonate the account this service is running under. Additionally, if UNC paths are used, there is no need to do a read operation on the named pipe before it is possible to impersonate the client end of the pipe.

This behavior is easy to exploit in Microsoft SQL Server since there are a large number of procedures where we can specify which file to use. As an example, we will use `xp_fileexist`, an extended stored procedure that public can execute. By creating a named pipe server with an arbitrary name and execute `xp_fileexist` with the UNC name of the named pipe as an argument, one can impersonate the user account SQL Server is running under.

Note that this is a system-wide behavior and not limited to Microsoft SQL Server.

See the section below for an easy to follow example, which describes the scenario.

Example:

Here follows a session which is cut-and-pasted from two command shells. `Mssqlpipe.exe` is a program that creates a named pipe, waits for a client to connect, and then impersonates the client. It then executes the program specified on the command line as the impersonated user.

From command shell #1:

```
C:\>mssqlpipe.exe cmd.exe
Creating pipe: \\.\Pipe\atstake
Pipe created, waiting for connection
Connect to the database (with isql for example) and execute:
xp_fileexist '\\SERVERNAME\pipe\atstake'
```

Then in command shell #2:

```
C:\>isql -U andreas
Password:
1> xp_fileexist '\\TEMP123\pipe\atstake'
2> go
File Exists File is a Directory Parent Directory Exists
```

1 0 1

Then, back in command shell #1:

Impersonate user successful, we are running as user: SYSTEM

Vendor Response:

Vendor first contacted on 06/21/2002

Vendor responded that they were working on fix: 07/08/2002

Vendor responded that fix would be in SP4: 10/02/2002

Vendor has fix in Windows 2000 SP4 available at:

<<http://www.microsoft.com/Windows2000/downloads/servicepacks/sp4/>>

<http://www.microsoft.com/Windows2000/downloads/servicepacks/sp4/>

Securiteam: [NT] Named Pipe Filename Local Privilege Escalation

The fix introduced a new user right in Windows 2000, "Impersonate a Client AfterAuthentication". This permission is only granted to Administrators and service accounts by default. More information is available in the Microsoft Knowledge Base:

<[http://support.microsoft.com/default.aspx?scid=kb;\[LN\];821546](http://support.microsoft.com/default.aspx?scid=kb;[LN];821546)>
[http://support.microsoft.com/default.aspx?scid=kb;\[LN\];821546](http://support.microsoft.com/default.aspx?scid=kb;[LN];821546)

@stake Recommendation:

If you are running Windows 2000 you should install SP4.

SQL Server 2000 can run as a less privileged account than SYSTEM which helps mitigate against this problem. Always configure your servers to run as the least privileged user account possible.

ADDITIONAL INFORMATION

The original advisory can be found at:

<<http://www.atstake.com/research/advisories/2003/a070803-1.txt>>
<http://www.atstake.com/research/advisories/2003/a070803-1.txt>

The information has been provided by <<mailto:advisories@atstake.com>>
@stake Advisories.

=====

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.