

[NT] Windows Local Security Authority Service Remote Buffer Overflow (MS04-011)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-04/0036.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 04/14/04

To: list@securiteam.com

Date: 14 Apr 2004 09:07:17 +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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Windows Local Security Authority Service Remote Buffer Overflow (MS04-011)

SUMMARY

eEye Digital Security has discovered a remote buffer overflow in the Windows LSA (Local Security Authority) Service (LSASRV.DLL). An unauthenticated attacker could exploit this vulnerability to execute arbitrary code with system-level privileges on Windows 2000 and Windows XP machines. The susceptible LSA functionality is accessible via the LSARPC named pipe over TCP ports 139 and 445.

This buffer overflow bug is within the Microsoft Active Directory service functions exposed by the LSASS DCE/RPC endpoint. These functions provide the ability to use Active Directory services both locally and remotely, and on default installations of Windows 2000 and Windows XP, no special privileges are required.

Some Active Directory service functions generate a debug log file in the "debug" subdirectory located in the Windows directory. A logging function implemented in LSASRV.DLL is called to write entries to the log file. In this function, the vsprintf() routine is used to create a log entry. The string arguments for this logging function are supplied as parameters to vsprintf() without any bounds checking, so if we can pass a long string

Securiteam: [NT] Windows Local Security Authority Service Remote Buffer Overflow (MS04-011)

argument to the logging function, then a buffer overflow will occur.

We found some RPC functions that will accept a long string as a parameter, and will attempt to write it to the debug log file. If we specify a long string as a parameter to these RPC functions, a stack-based buffer overflow will happen in the Active Directory service functions on the remote system. Attackers who successfully leverage this vulnerability will be executing code under the SYSTEM context of the remote host.

DETAILS

Affected Software:

* Microsoft Windows NT? Workstation 4.0 Service Pack 6a –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=7F1713FC-F95C-43E5-B825-3CF72C1A0A3E&dis>

Download the update

* Microsoft Windows NT Server 4.0 Service Pack 6a –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=67A6F461-D2FC-4AA0-957E-3B8DC44F9D79&dis>

Download the update

* Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6

–

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=62CBA527-A827-4777-8641-28092D3AAE4F&dis>

Download the update

* Microsoft Windows 2000 Service Pack 2, Microsoft Windows 2000 Service Pack 3, and Microsoft Windows 2000 Service Pack 4 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=0692C27E-F63A-414C-B3EB-D2342FBB6C00&dis>

Download the update

* Microsoft Windows XP and Microsoft Windows XP Service Pack 1 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=3549EA9E-DA3F-43B9-A4F1-AF243B6168F3&dis>

Download the update

* Microsoft Windows XP 64-Bit Edition Service Pack 1 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=C6B55EF2-D9FE-4DBE-AB7D-73A20C82FF73&d>

Download the update

* Microsoft Windows XP 64-Bit Edition Version 2003 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=C207D372-E883-44A6-A107-6CD2D29FC6F5&dis>

Download the update

* Microsoft Windows Server 2003 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=EAB176D0-01CF-453E-AE7E-7495864E8D8C&dis>

Download the update

* Microsoft Windows Server 2003 64-Bit Edition –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=C207D372-E883-44A6-A107-6CD2D29FC6F5&dis>

Download the update

* Microsoft NetMeeting

* Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (ME) – Review the FAQ section of this bulletin for details about these operating systems.

Technical Description:

The buffer overflow bug is in a logging function which generates a string for the log file using vsprintf(). The name of the log file is "DCPROMO.LOG", and it is located in the Windows "debug" directory.

Securiteam: [NT] Windows Local Security Authority Service Remote Buffer Overflow (MS04-011)

The Active Directory service functions implemented in LSASRV.DLL are as follows:

Function number – Function Name

0 DsRolerGetPrimaryDomainInformation
1 DsRolerDnsNameToFlatName
2 DsRolerDcAsDc
3 DsRolerDcAsReplica
4 DsRolerDemoteDc
5 DsRolerGetDcOperationProgress
6 DsRolerGetDcOperationResults
7 DsRolerCancel
8 DsRolerServerSaveStateForUpgrade
9 DsRolerUpgradeDownlevelServer
10 DsRolerAbortDownlevelServerUpgrade

In these functions, the DsRolepInitializeLog() API is called to create the log file "DCPROMO.LOG" in the Windows "debug" subdirectory. After calling this API, entries are written to the log file by invoking the DsRolepLogPrintRoutine() function. The following is an example of a log file that can be generated on the remote host using DsRolerDcAsDc() API:

```
09/25 21:49:22 [INFO] DsRolerDcAsDc: DnsDomainName aaaaa  
09/25 21:49:22 [INFO] SiteName bbbbb  
09/25 21:49:22 [INFO] SystemVolumeRootPath ccccc  
09/25 21:49:22 [INFO] DsDatabasePath ddddd, DsLogPath eeeee  
09/25 21:49:22 [INFO] ParentDnsDomainName fffff  
09/25 21:49:22 [INFO] ParentServer ggggg  
09/25 21:49:22 [INFO] Account hhhhh  
09/25 21:49:22 [INFO] Options 1
```

The remote host can be specified as the first argument of the DsRolerDcAsDc() API. The parameters shown in this debug log file such as DnsDomainName "aaaaa", SiteName "bbbb", and SystemVolumeRootPath "cccc" are string arguments for the DsRolerDcAsDc() API. These string parameters are logged using DsRolepLogPrintRoutine(), so, we can cause a buffer overflow condition by supplying a long DnsDomainName, SiteName, SystemVolumeRootPath, etc.

However, most of Active Directory service functions call RpcImpersonateClient() API, which changes the server thread's security context to that of the client. Generally, the "debug" subdirectory located in the Windows directory is not writeable by everyone if the drive is formatted as NTFS, meaning that we cannot append to the log using a null session. The RpcImpersonateClient() API is called before opening the log file, and if the connected client does not have the privilege to write to the log file, then CreateFile() will fail, and the vulnerable call to vsprintf() is not performed.

Securiteam: [NT] Windows Local Security Authority Service Remote Buffer Overflow (MS04-011)

However, the `DsRolerUpgradeDownlevelServer()` function, which is supported by Windows 2000 and XP, does not use the `RpcImpersonateClient()` API — it calls `DsRolepInitializeLog()` API immediately. So, if we specify a long string parameter to this function, we can pass these parameters into `vsprintf()` in the `DsRolepLogPrintRoutine()` API, and a buffer overflow will occur.

The `DsRoleUpgradeDownlevelServer()` client API which issues the DCE/RPC request is implemented in `NETAPI32.DLL`. This is an undocumented API. If we specify a long `szDomainName`, `LSASS.EXE` — which provides the Active Directory service functions running on the local computer — will crash. This type of attack can be performed against the local machine for the purpose of privilege escalation.

There is no parameter to specify the remote host for the `DsRoleUpgradeDownlevelServer()` client API. The API specifies the host as `NULL` internally, so the DCE/RPC request will be sent to `LSASS.EXE` running on the local computer. However, the function called from `LSASS.EXE` does not check whether the request is sent from the local machine or a remote one, so it will also handle requests sent from remote hosts. So, if we craft this DCE/RPC packet by hand, or if we modify the client API to be able to specify remote host, then we can cause a buffer overflow on an arbitrary remote host running Windows 2000 or Windows XP.

Because the Active Directory services interface is registered on the `LSASS` named pipe RPC endpoint (`ncacn_np:host[\PIPE\LSARPC]`), it is sufficient to use `CreateFile()` and `ReadFile()`, `WriteFile()`, and/or `TransactNamedPipe()` in order to communicate with `LSASS.EXE` on the vulnerable host. No SMB knowledge is necessary, just an RPC bind and a `DsRoleUpgradeDownlevelServer()` packet.

We also can craft this DCE/RPC packet if we modify the instructions of `DsRoleUpgradeDownlevelServer()` client API. The first argument for `DsRolepEncryptPasswordStart()` API which is used in `DsRoleUpgradeDownlevelServer()` API internally is the remote host. In this case, `NULL` is specified for the first argument. So, if we can change this to the pointer which is stored the remote host, we can send DCE/RPC request for `DsRoleUpgradeDownlevelServer()` function.

In order to modify the `DsRoleUpgradeDownlevelServer()` API, the protections on a region of this API implemented in `NETAPI32.DLL` must be changed to `PAGE_EXECUTE_READWRITE` using the `VirtualProtect()` API. The following code changes will allow the remote host to be specified as the 9th parameter (`szUnknown2`) of the `DsRoleUpgradeDownlevelServer()` API.

In case of Windows 2000, we should specify the `DomainName` as Unicode; on Windows XP, we should use ASCII. We can execute about 2KB of code on the remote host using this buffer overflow.

Vendor Status:

Microsoft has released a patch for this vulnerability. The patch is

Securiteam: [NT] Windows Local Security Authority Service Remote Buffer Overflow (MS04-011)

available at:

<<http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx>>
<http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx>.

ADDITIONAL INFORMATION

The information has been provided by <mailto:mmaiffret@EEYE.COM> Marc Maiffret.

=====

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.