

[NT] Microsoft NetDDE Service Unauthenticated Remote Buffer Overflow (MS04-031)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0088.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 01/23/05

To: list@securiteam.com

Date: 23 Jan 2005 14:37:11 +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>

Microsoft NetDDE Service Unauthenticated Remote Buffer Overflow (MS04-031)

SUMMARY

A vulnerability has been discovered in the Microsoft NetDDE service that allows a remote attacker to execute arbitrary code on a system without authentication. This vulnerability can also be used by any low privileged local user to gain Local System privileges.

DETAILS

The NetDDE (Network Dynamic Data Exchange) services are designed to be used by network applications as a method of interprocess communication. NetDDE achieves this by allowing individual applications to create and maintain machine resource shares, through which data is dynamically exchanged. When a new share is created, the NetDDE DSDM (DDE Share Database Manager) service is used to store the share information.

To control access to the DDE shares which have been created, NetDDE exports a set of functions which can be used to grant 'trusted' status to a particular share. Only the user who has created the share can grant trusted status to the share, and without a user granting trusted status to the share it is not possible for a NetDDE client to exchange data with the

application using that share.

It is in the code which is designed to set trusted status to a share that the vulnerability can be found.

Technical Details:

The function exported by NetDDE to grant trusted status to a share is as follows:

```
UINT NDdeSetTrustedShare(  
~ LPTSTR lpszServer,  
~ LPTSTR lpszShareName,  
~ DWORD dwTrustOptions  
);
```

The first parameter, `lpszServer`, specifies the name of the server on which the NetDDE and DSDM service reside. The second parameter, `lpszShareName`, is the name of the share which is to gain the trusted status. The third parameter, `dwTrustOptions`, describes the operation (or level of trust) which is to be performed upon the share. NetDDE maintains a list of trusted shares in the system registry which is modified upon the successful execution of a 'set trusted share' request. When attempting to construct an absolute registry path upon which to operate, the `lpszShareName` string value is concatenated onto the trusted share root path into a stack based buffer. Since no boundary checking is performed during this operation, it is a trivial matter to overflow this buffer and overwrite an arbitrary quantity of the stack – including the saved return address.

When observing a `NDdeSetTrustedShare()` function call being made to a remote NetDDE server, it can be seen that the call will fail unless an authenticated session has already been established with the target machine – by default a null session is not sufficient.

During further research of the vulnerability, we observed that there was a difference in the network interactions between an application communicating with a NetDDE server, and two NetDDE servers communicating with each other. We discovered that when two NetDDE servers needed to communicate, NetBIOS, instead of SMB was the means of transport for the data which was to be passed over the network. Furthermore, all that was required for the two NetDDE services to establish communication in this fashion was a NetBIOS session setup request.

Further investigation showed that an attacker could simply interact with the vulnerable function over NetBIOS in this fashion without first needing to successfully complete the authentication stage necessary to communicate with the NetDDE named pipe. Communicating directly in this manner grants the attacker remote, unauthenticated access to the vulnerable function.

Fix Information:

Microsoft have released an update for NetDDE which addresses this issue. This can be downloaded from:

Securiteam: [NT] Microsoft NetDDE Service Unauthenticated Remote Buffer Overflow (MS04-031)

<<http://www.microsoft.com/technet/security/bulletin/MS04-031.msp>>
<http://www.microsoft.com/technet/security/bulletin/MS04-031.msp>.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:nisr@nextgenss.com>>
NGSSoftware Insight Security Research.

The original article can be found at:

<<http://www.ngssoftware.com/advisories/netddefull.txt>>
<http://www.ngssoftware.com/advisories/netddefull.txt>

=====

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.