

[NT] Unchecked Buffer in Locator Service Could Lead to Code Execution

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-01/0067.html>

From: support@securiteam.com

Date: 01/23/03

From: support@securiteam.com

To: list@securiteam.com

Date: 23 Jan 2003 17:42:05 +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 would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit http://www.worldonline.co.za/services/work_ip.asp

Unchecked Buffer in Locator Service Could Lead to Code Execution

SUMMARY

The Microsoft Locator service is a name service that maps logical names to network-specific names. It ships with Windows NT 4.0, Windows 2000, and Windows XP. By default, the Locator service is enabled only on Windows 2000 domain controllers and Windows NT 4.0 domain controllers; it is not enabled on Windows NT 4.0 workstations or member servers, Windows 2000 workstations or member servers, or Windows XP.

A security vulnerability results from an unchecked buffer in the Locator service. By sending an especially malformed request to the Locator service, an attacker could cause the Locator service to fail, or to run code of the attacker's choice on the system.

DETAILS

Affected Software:

- * Microsoft Windows NT 4.0
- * Microsoft Windows NT 4.0, Terminal Server Edition
- * Microsoft Windows 2000
- * Microsoft Windows XP

Securiteam: [NT] Unchecked Buffer in Locator Service Could Lead to Code Execution

Mitigating factors:

* The Locator service is not enabled by default on any affected versions of Windows with the exception of Windows 2000 domain controllers and Windows NT 4.0 domain controllers.

* A properly-configured firewall would block the calls to the Locator service, which would protect an affected machine from an Internet-based attack.

Patch availability:

Download locations for this patch

* Windows NT 4.0:

*

<<http://microsoft.com/downloads/details.aspx?FamilyId=F92D1E86-590A-4DA5-93F2-FCC6300A1A43&displaylang=en>>
except Japanese NEC and Chinese – Hong Kong

*

<<http://microsoft.com/downloads/details.aspx?FamilyId=F211C932-D442-4A1A-B385-77975DE3B280&displaylang=en>>
NEC

*

<<http://microsoft.com/downloads/details.aspx?FamilyId=C8AAB17B-48B2-4E9F-B06F-2A54BA59A45F&displaylang=en>>
– Hong Kong

* Windows NT 4.0, Terminal Server Edition:

*

<<http://microsoft.com/downloads/details.aspx?FamilyId=EB651162-97F2-47F9-8E99-016B35B7646D&displaylang=en>>

* Windows 2000:

*

<<http://microsoft.com/downloads/details.aspx?FamilyId=33FF827A-D5DB-4F92-9DEF-4D91A140E0E0&displaylang=en>>
except Japanese NEC

*

<<http://microsoft.com/downloads/details.aspx?FamilyId=1B142CF9-CADA-4DFF-B42D-7E2022A17E6A&displaylang=en>>
NEC

* Windows XP:

*

<<http://microsoft.com/downloads/details.aspx?FamilyId=DF24197E-6217-4ABD-A244-0A53320B2813&displaylang=en>>
Edition

*

<<http://microsoft.com/downloads/details.aspx?FamilyId=B8999D16-3DAD-4E20-B46E-E1AEFB1F6673&displaylang=en>>
Edition

What's the scope of the vulnerability?

This is a buffer overrun vulnerability. An attacker who successfully exploited this vulnerability could cause the Locator service to fail, or could cause code of the attacker's choice to be executed with system privileges.

The Locator service is not enabled by default except on Windows 2000 domain controllers and Windows NT 4.0 domain controllers. A properly-configured firewall would block the calls to the Locator service,

Securiteam: [NT] Unchecked Buffer in Locator Service Could Lead to Code Execution

which would protect an affected machine from an Internet-based attack.

What causes the vulnerability?

The vulnerability results because of an unchecked buffer in the Microsoft Locator service. If the Locator service was called using a specially malformed argument, it could have the effect of overrunning the buffer.

What is the Locator service?

The Microsoft Locator service is a name service that maps names to objects. The name is a logical name that is easy for users to recognize and use. The Locator service ships with Windows NT 4.0, Windows 2000, and Windows XP.

What is the Locator service used for?

A client that is going to make a Remote Procedure Call (RPC) can call the Locator service to resolve a logical name for a network object to a network-specific name for use in the RPC. For example, if a print server has the logical name "laserprinter", an RPC client could call the Locator service to find out the network-specific name that mapped to "laserprinter". The RPC client uses the network-specific name when it makes the RPC call to the service.

By default, the Locator service is only enabled on Windows 2000 domain controllers and Windows NT 4.0 domain controllers. An administrator could enable the Locator service on any Windows NT 4.0, Windows 2000, or Windows XP system.

What is a Remote Procedure Call?

A Remote Procedure Call is an interprocess communication technique that allows client/server software to communicate. RPC can be used in client/server applications based on Microsoft Windows operating systems and can be used in heterogeneous network environments that include other operating systems.

What's wrong with Locator service?

There is a flaw in the way the Locator service handles certain parameter information that is passed to it. An especially malformed parameter data could be passed to the Locator service and could cause a buffer to be overrun.

What could this vulnerability enable an attacker to do?

If an attack were successful, this vulnerability could enable an attacker to cause the Locator service to fail, or to be able to run code on the system.

How could an attacker exploit this vulnerability?

An attacker could seek to exploit this vulnerability by forming an RPC call that would employ the Locator service to resolve a logical name, and using the RPC call to pass especially malformed data.

Securiteam: [NT] Unchecked Buffer in Locator Service Could Lead to Code Execution

Because a properly configured firewall that blocked NetBIOS traffic would block access to the Locator service from the Internet, a successful attack would need to be launched from an organization's internal network.

Does the Locator service require authentication?

No, the system making the RPC request does not have to be authenticated by the system running the Locator service.

Could this vulnerability be exploited from the Internet?

A properly-configured firewall would block the calls to the Locator service, which would protect an affected machine from an Internet-based attack. An attacker would be much more likely to attempt to exploit this vulnerability from an organization's internal network.

How do I tell if the Locator service is enabled?

The status of the "Remote Procedure Call (RPC) Locator" service and how it is started (automatically or manually) can be viewed in the Control Panel. For Windows 2000 and Windows XP, use Control Panel | Administrative Tools | Services, and on Windows NT 4.0, use Control Panel | Services.

It is also possible to determine the status of the Locator service from the command line by entering:

```
net start
```

A list of services will be displayed. If "Remote Procedure Call (RPC) Locator" appears in the list, then the locator service is running.

If I am not using the Locator service, can I disable it?

Yes. An administrator can disable the Locator service by setting the RpcLocator service status to "disabled" in the services control panel.

The service can also be stopped via the command line using the sc.exe program, which ships with Windows XP and is included as part of the Windows 2000 Resource Kit. The following command will stop the service:

```
sc stop RpcLocator
```

To disable the service using the command line tool, use the following:

```
sc config RpcLocator start= disabled
```

What systems would be at greatest risk from this vulnerability?

Only Windows 2000 domain controllers and Windows NT 4.0 domain controllers have the Locator service enabled by default, so those would be the systems at greatest risk. The Locator service can be enabled on Windows NT 4.0, Windows NT 4.0, Terminal Server Edition, Windows 2000, and Windows XP.

What does the patch do?

The patch addresses the vulnerability by correctly handling the information passed to the RPC Locator service.

ADDITIONAL INFORMATION

Securiteam: [NT] Unchecked Buffer in Locator Service Could Lead to Code Execution

The information has been provided by

<mailto:0_43313_E51E4D7D-DECD-43AE-9A29-36080E8D4C3C_US@Newsletters.Microsoft.com>

Microsoft Product Security.

=====

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.