

[NT] Flaw in Windows Function Could Allow Denial of Service

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-07/0104.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 07/24/03

To: list@securiteam.com

Date: 24 Jul 2003 16:38:41 +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

Flaw in Windows Function Could Allow Denial of Service

SUMMARY

A flaw exists in a Windows NT 4.0 Server file management function that can cause a denial of service vulnerability.

The flaw results because the affected function can cause memory that it does not own to be freed when a specially crafted request is passed to it.

If the application making the request to the function does not carry out any user input validation and allows the specially crafted request to be passed to the function, the function may free memory that it does not own. As a result, the application passing the request could fail.

By default, the affected function is not accessible remotely, however applications installed on the operating system that are available remotely may make use of the affected function.

Application servers or Web servers are two such applications that may access the function.

Securiteam: [NT] Flaw in Windows Function Could Allow Denial of Service

Note that Internet Information Server 4.0 (IIS 4.0) does not, by default, make use of the affected function.

DETAILS

Vulnerable Systems:

- * Microsoft Windows NT 4.0 Server
- * Microsoft Windows NT 4.0 Terminal Server Edition

Immune Systems:

- * Microsoft Windows 2000
- * Microsoft Windows XP
- * Microsoft Windows Server 2003

Mitigating factors:

- * The default installation of Windows NT 4.0 Server is not vulnerable to a remote denial of service. Additional software that makes use of the affected file management function must be installed on the system to expose the vulnerability remotely.
- * If the application calling the affected file management function carries out input validation, the specially crafted request may not be passed to the vulnerable function.
- * The vulnerability cannot be used to cause Windows NT 4.0 Server itself to fail. Only the application that makes the request may fail.

Frequently asked questions

What's the scope of the vulnerability?

This is a denial of service vulnerability. An attacker who successfully exploited the vulnerability could cause an application running on a Windows NT 4.0 Server system to fail. By default the vulnerable function cannot be accessed remotely, however, additional software that may have been installed on the server may make the function accessible remotely.

What causes the vulnerability?

The vulnerability results because of a flaw in the way certain memory operations relating to a Windows function are carried out by Windows NT 4.0 Server.

Which Windows function is vulnerable?

The file management function is vulnerable. Therefore, the vulnerability is only exposed by applications that make use of this function.

What's wrong with the way the Windows NT 4.0 Server file management function carries out memory operations?

There is a flaw in the way a Windows function handles memory operations. If a specially crafted request is made to the affected function, the server may incorrectly free some memory that is not actually owned by the function. This could cause the application making the overly long request to fail.

Securiteam: [NT] Flaw in Windows Function Could Allow Denial of Service

What could this vulnerability enable an attacker to do?

This vulnerability could enable an attacker to cause an application running on Windows NT 4.0 Server to fail. The application that could fail would be the application that was making use of the affected function and that was allowing the specially crafted request to be passed to the API.

What types of applications might make a request to the vulnerable function?

Typically applications that require information about the file system might make requests to the function. Such applications might include Web servers or application servers. Note that Microsoft Internet Information Server 4.0 (IIS 4.0) does not make use of the function and cannot therefore be used to exploit the vulnerability.

How could an attacker exploit this vulnerability?

An attacker could seek to exploit this vulnerability by sending a specially crafted request to the affected function by using another application. If the application making the request does not carry out any user input validation, the affected function may then free memory that it does not own, causing the calling application to fail.

What does the patch do?

The patch eliminates the vulnerability by ensuring that the affected component does not free memory that it does not own.

Patch availability

*

<http://microsoft.com/downloads/details.aspx?FamilyId=8FF8CA3E-D546-4FAF-851F-FFBE2490B901&displaylang=en>

Microsoft Windows NT 4.0 Server

*

<http://microsoft.com/downloads/details.aspx?FamilyId=5C46460D-3887-4D5F-B142-F505BB208797&displaylang=en>

Microsoft Windows NT 4.0 Terminal Server Edition

Support:

* Microsoft Knowledge Base article

<http://support.microsoft.com/?kbid=823803> 823803 discusses this issue and will be available approximately 24 hours after the release of this bulletin. Knowledge Base articles can be found on the Microsoft Online Support web site.

* Technical support is available from Microsoft Product Support Services. There is no charge for support calls associated with security patches.

ADDITIONAL INFORMATION

Vulnerability discovered by Matt Miller and Jeremy Rauch of

<http://atstake.com> @stake

Original article can be found at:

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-029.asp>
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-029.asp>

Securiteam: [NT] Flaw in Windows Function Could Allow Denial of Service

=====

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.