

Securiteam: [NT] Authentication Flaw in Windows Debugger can lead to Elevated Privileges

[NT] Authentication Flaw in Windows Debugger can lead to Elevated Privileges

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-05/0094.html>

From: support@securiteam.com

Date: 05/23/02

From: support@securiteam.com

To: list@securiteam.com

Date: Thu, 23 May 2002 08:44:09 +0200 (CEST)

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.

Authentication Flaw in Windows Debugger can lead to Elevated Privileges

SUMMARY

The Windows debugging facility provides a means for programs to perform diagnostic and analytic functions on applications as they are running on the operating system. One of these capabilities allows for a program, usually a debugger, to connect to any running program, and to take control of it. The program can then issue commands to the controlled program, including the ability to start other programs. These commands would then execute in the same security context as the controlled program.

There is a flaw in the authentication mechanism for the debugging facility such that an unauthorized program can gain access to the debugger. A vulnerability results because an attacker can use this to cause a running program to run a program of her choice. Because many programs run as the operating system, this means that an attacker can exploit this vulnerability to run code as the operating system itself. She could take any action on the system including deleting data, adding accounts with administrative access, or reconfiguring the system.

A successful attack requires the ability to logon interactively to the system, either at the console or through a terminal session. Also, a successful attack requires the introduction of code to exploit this

Securiteam: [NT] Authentication Flaw in Windows Debugger can lead to Elevated Privileges

vulnerability. Because best practices recommends restricting the ability to logon interactively on servers, this issue most directly affects client systems and terminal servers.

DETAILS

Affected Software:

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

Mitigating factors:

* A successful attack requires the ability to logon interactively to the target machine, either directly at the console or through a terminal session. Best practices strongly militate against ever allowing an unprivileged user to interactively log onto business-critical systems such as ERP servers, database servers, domain controllers and the like. If these recommendations have been followed, the vulnerability would principally pose a threat only to systems like workstations and terminal servers.

* A successful attack requires that the attacker be able to load code of her choice on the system. Restrictions on a user's ability to load and execute arbitrary code could potentially prevent a successful attack.

Patch availability:

Download locations for this patch

- * Windows NT 4.0:

<<http://www.microsoft.com/ntserver/nts/downloads/security/q320206/default.asp>>

<http://www.microsoft.com/ntserver/nts/downloads/security/q320206/default.asp>

- * Windows NT 4.0 Terminal Server Edition:

<<http://www.microsoft.com/ntserver/terminalserver/downloads/security/Q320206/default.asp>>

<http://www.microsoft.com/ntserver/terminalserver/downloads/security/Q320206/default.asp>

- * Windows 2000:

<<http://www.microsoft.com/windows2000/downloads/security/q320206/default.asp>>

<http://www.microsoft.com/windows2000/downloads/security/q320206/default.asp>

What's the scope of the vulnerability?

This is a privilege elevation vulnerability. A malicious user who has the ability to interactively log on to a system and run code of her choice could seek to exploit this vulnerability and pose as any user on the system, including any administrator or the operating system itself.

Because this requires the ability to logon interactively and run a program, the systems most likely to be affected by this vulnerability are client systems and terminal servers, which regularly allow end-users access to the system directly at the keyboard. Internet servers, file and print servers, and application servers such as SQL servers usually restrict the ability to logon interactively, and thus are less likely to

Securiteam: [NT] Authentication Flaw in Windows Debugger can lead to Elevated Privileges

be affected by this vulnerability.

What causes the vulnerability?

The vulnerability results because of a flaw in how access to the debugging facility in Windows is validated. Due to a flaw in how requests to attach to the system debugger are authenticated, it's possible for unauthorized programs to gain access to it.

What is the debugging facility in Windows?

The debugging facility in Windows provides a way for system administrators and developers to troubleshoot programs running on Windows.

The Windows debugging facility differs from those found in development environments such as Visual Studio in that it allows for viewing and analysis of the code as it is running on the operating system in real-time. This can help developers and engineers to view and diagnose issues that are specific to a particular machine or configuration by allowing them to interrogate the code directly on the system.

How does the Windows debugging facility work?

At the root of the ability to debug code when running is the ability for one program to "attach" to another. In almost every case, this will be a debugging program or debugger that then connects or "attaches" to the running program, or debuggee.

"Attaching" provides the means by which the debugger can then control the program being debugged. Since the process of troubleshooting requires the ability for the debugger to completely manipulate the debuggee program, the debugging facility grants the debugger the same level of control over the running program as it has itself.

What's wrong with the debugging facility in Windows?

Before allowing a debugger to attach to another program, the Windows debugger ensures that the debugger has the appropriate privileges. However, there is a flaw in how the authentication is performed, with the result that a program could be able to attach to the debugger without having the proper privileges to do so.

What could this vulnerability enable an attacker to do?

One of the capabilities that the debugger grants to applications that attach to running programs is the ability to command the running program to in turn launch new programs. When these programs are launched, they run in the security context of the launching program.

This means that this vulnerability could allow an attacker to run a program of her choosing on the system with the same privileges as any other program currently running on the system. Since a number of programs run on the system in the context of the operating system, an attacker could use this vulnerability to make her program run as if it were the operating system.

Securiteam: [NT] Authentication Flaw in Windows Debugger can lead to Elevated Privileges

A program run in this security context would have complete control over the machine and would be able to take any action that the operating system itself could take. This includes but is not limited to adding accounts with administrative privileges, deleting critical system files, and changing security settings.

How could an attacker exploit this vulnerability?

An attacker could seek to exploit this vulnerability by writing a program that would attempt to connect to the debugging facility in Windows in a way that exploits this flaw. The attacker would most likely have her program then attempt to connect to a well-known program that runs with SYSTEM level privileges and command that program to launch a program of her choice.

Because this cannot be exploited without the ability to logon and the ability to introduce hostile code to the system, best practices that limit users' ability to logon and load programs, in accordance with the rule of least privilege, can mitigate against the chances for a successful attack.

Would this give an attacker control over the network?

In most cases, this would not. However, it will depend on the machine on which a user has logon rights. For example, if an unprivileged user were able to logon to a domain control and exploit this vulnerability, she could use this to achieve administrative privileges on the domain itself.

However, because domain controllers contain sensitive, network-wide information like this, they are usually configured in accordance with least privilege best practices and, thus, non-administrative users do not have the ability to interactively logon to them.

What does the patch do?

The patch eliminates the vulnerability by implementing proper validation for requests to attach to the debugging system.

ADDITIONAL INFORMATION

The information has been provided by

<mailto:0_31573_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

=====

=====

Securiteam: [NT] Authentication Flaw in Windows Debugger can lead to Elevated Privileges

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.

- **Previous message:** support@securiteam.com: "[NT] Multiple vulnerabilities in New Atlanta ServletExec ISAPI"
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)