

[NT] Vulnerability in Microsoft Jet Database Engine Allows Code Execution (MS08-028)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-05/msg00018.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 15 May 2008 19:26:13 +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>

Vulnerability in Microsoft Jet Database Engine Allows Code Execution
(MS08-028)

SUMMARY

This security update resolves a security vulnerability in the Microsoft Jet Database Engine (Jet) in Windows. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

DETAILS

Affected Software:

* Microsoft Windows 2000 Service Pack 4 –

<<http://www.microsoft.com/downloads/details.aspx?familyid=0de12d09-e675-4cf0-bc6f-e42eeb4784a1>>

Microsoft Jet 4.0 Database Engine – Remote Code Execution – Critical – MS04-014

* Windows XP Service Pack 2 –

<<http://www.microsoft.com/downloads/details.aspx?familyid=3247433f-0aa9-49b8-9e40-c5463a95bcff>>

Microsoft Jet 4.0 Database Engine – Remote Code Execution – Critical – None

* Windows XP Professional x64 Edition –

[NT] Vulnerability in Microsoft Jet Database Engine Allows Code Execution (MS08-028)

<<http://www.microsoft.com/downloads/details.aspx?familyid=4915ebc4-5e7b-493e-b8c4-321d40d9a701>>

Microsoft Jet 4.0 Database Engine – Remote Code Execution – Critical – None

* Windows Server 2003 Service Pack 1 –

<<http://www.microsoft.com/downloads/details.aspx?familyid=86e3ed62-98f7-46ec-96ab-5e8c123b1288>>

Microsoft Jet 4.0 Database Engine – Remote Code Execution – Critical – None

* Windows Server 2003 x64 Edition –

<<http://www.microsoft.com/downloads/details.aspx?familyid=5dfc867b-74b7-4818-9fc2-d71e7c9d2e38>>

Microsoft Jet 4.0 Database Engine – Remote Code Execution – Critical – None

* Windows Server 2003 with SP1 for Itanium-based Systems –

<<http://www.microsoft.com/downloads/details.aspx?familyid=3452119b-ba4c-4272-82ec-97396b2c2c3d>>

Microsoft Jet 4.0 Database Engine – Remote Code Execution – Critical – None

Non-Affected Software:

* Windows XP Professional x64 Edition Service Pack 2 – Microsoft Jet 4.0 Database Engine

* Windows XP Service Pack 3 – Microsoft Jet 4.0 Database Engine

* Windows Server 2003 Service Pack 2 – Microsoft Jet 4.0 Database Engine

* Windows Server 2003 x64 Edition Service Pack 2 – Microsoft Jet 4.0 Database Engine

* Windows Server 2003 with SP2 for Itanium-based Systems – Microsoft Jet 4.0 Database Engine

* Windows Vista and Windows Vista Service Pack 1 – Microsoft Jet 4.0 Database Engine

* Windows Vista for x64-based Systems and Windows Vista Service Pack 1 for x64-based Systems – Microsoft Jet 4.0 Database Engine

* Windows Server 2008 for 32-bit Systems – Microsoft Jet 4.0 Database Engine

* Windows Server 2008 for x64-based Systems – Microsoft Jet 4.0 Database Engine

* Windows Server 2008 for Itanium-based Systems – Microsoft Jet 4.0 Database Engine

Microsoft Jet Engine MDB File Parsing Stack Overflow Vulnerability – CVE-2007-6026

A buffer overrun vulnerability exists in the Microsoft Jet Database Engine (Jet) that could allow remote code execution on an affected system. An attacker could exploit the vulnerability by creating a specially crafted database query and sending it through an application that is using Jet on an affected system. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

Mitigating Factors for Microsoft Jet Engine MDB File Parsing Stack Overflow Vulnerability – CVE-2007-6026

Mitigation refers to a setting, common configuration, or general best-practice, existing in a default state, that could reduce the severity of exploitation of a vulnerability. The following mitigating factors may be helpful in your situation:

* An attacker who successfully exploited this vulnerability could gain the same user rights as the local user. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

* In a Web-based attack scenario, an attacker would have to host a Web site that contains a specially crafted Word file that is used to attempt to exploit this vulnerability. In addition, compromised Web sites and Web sites that accept or host user-provided content could contain specially crafted content that could exploit this vulnerability. An attacker would have no way to force users to visit these Web sites. Instead, an attacker would have to persuade users to visit the Web site, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users to the attacker's site.

* Systems that use Microsoft Outlook 2003 and 2007 as their e-mail client can mitigate the HTML email vector for Outlook 2007 by configuring mail to be read in plain text only.

* Systems running all supported editions of Windows XP Service Pack 3, Windows Server 2003 Service Pack 2, Windows Vista, and Windows Server 2008 are not affected by this vulnerability.

Workarounds for Microsoft Jet Engine MDB File Parsing Stack Overflow Vulnerability – CVE–2007–6026

Workaround refers to a setting or configuration change that does not correct the underlying vulnerability but would help block known attack vectors before you apply the update. Microsoft has tested the following workarounds and states in the discussion whether a workaround reduces functionality:

* Restrict the Microsoft Jet Database Engine from running for any application

To implement the workaround, enter the following command at a command prompt:

```
echo y| cacls "%SystemRoot%\system32\msjet40.dll" /E /P everyone:N
```

Impact of workaround. Any application requiring the use of the Microsoft Jet Database Engine to make data access calls will not function.

How to undo the workaround. Enter the following command at a command prompt

```
echo y| cacls "%SystemRoot%\system32\msjet40.dll" /E /R everyone
```

* Use group policy to restrict the Microsoft Jet Database Engine from running for any application

[NT] Vulnerability in Microsoft Jet Database Engine Allows Code Execution (MS08–028)

To implement the workaround, perform the following steps:

1. Create the following script, named JetCacls.cmd for illustration:

```
@echo off
if exist %systemdrive%\Cacls.log goto end
cacls "%SystemRoot%\system32\msjet40.dll" /E /P everyone:N > nul 2>&1
echo %date% %time%: Msjet Cacls updated > %systemdrive%\Cacls.log
:end
exit
```

2. Copy JetCacls.cmd to the Netlogon shared folder, or another shared folder on the domain controller from which JetCacls.cmd would run.

3. Set up JetCacls.cmd. In the Active Directory Users and Computers MMC snap-in, right-click the domain name, and then click Properties.

4. Click the Group Policy tab.

5. Click New to create a new Group Policy object (GPO), and enter JetCacls for the name of the policy.

6. Click the new policy, and then click Edit.

7. Expand Windows Settings for Computer Configuration, and then click Scripts.

8. Double-click Logon, and then click Add. The Add a Script dialog box appears.

9. Type \\servername\sharename\JetCacls.cmd in the Script Name box.

10. Click OK, and then click Apply.

11. Then restart the client computers that are members of this domain.

Impact of workaround. Any application that requires the use of the Microsoft Jet Database Engine to make data access calls will not function. This restriction only applies to applications that are running on client computers in the domain.

* Block MDB files from being processed through your mail infrastructure

Note All Jet database files should be treated as unsafe file types for common users and Microsoft recommends that database files transferred via e-mail be treated as suspicious.

To implement this workaround, your mail environment must support the ability to search for attachments containing a specific file structure (not just the file extension) within an e-mail message and then perform actions on the attachment such as delete, quarantine, notify, and report

[NT] Vulnerability in Microsoft Jet Database Engine Allows Code Execution (MS08-028)

the detected file.

To detect Jet files that have possibly been renamed to another file type, search for files with any of the following 15-byte signatures at location 0x4 (no quotes):

"Jet System DB "
"Standard Jet DB"
"Temp Jet DB "

For configurations specific to Microsoft Exchange customers using Forefront (formerly Antigen) technologies, please see Microsoft Forefront Server Security: File Filtering for more information.

This information has been shared with members of Microsoft Security Response Alliance. To utilize the MSRA tools to detect MDB files, please contact the providers as listed on the MSRA home page.

Impact of Workaround. Files detected by this configuration will be blocked from processing through an organization's e-mail system.

* Configure Outlook 2007 to read mail in plain text.

* Do not open or save Jet or Microsoft Word files that you receive from untrusted sources or that you receive unexpectedly from trusted sources. This vulnerability could be exploited when a user opens a specially crafted file.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6026>>
CVE-2007-6026

ADDITIONAL INFORMATION

The information has been provided by Microsoft Product Security.

The original article can be found at:

<<http://www.microsoft.com/technet/security/Bulletin/ms08-028.msp>>
<http://www.microsoft.com/technet/security/Bulletin/ms08-028.msp>

=====

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@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====
=====

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.