

[NT] Vulnerability in Microsoft Malware Protection Engine Allows Code Execution (MS07-010)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-02/msg00040.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 15 Feb 2007 12:08:35 +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 Malware Protection Engine Allows Code Execution
(MS07-010)

SUMMARY

A remote code execution vulnerability exists in the Microsoft Malware Protection Engine because of the way that it parses Portable Document Format (PDF) files. An attacker could exploit the vulnerability by constructing a specially crafted PDF File that could potentially allow remote code execution when the target computer system receives, and the Microsoft Malware Protection Engine scans, the PDF file.

DETAILS

Affected Software:

- * Windows Live OneCare
- * Microsoft Antigen for Exchange 9.x
- * Microsoft Antigen for SMTP Gateway 9.x
- * Microsoft Windows Defender
- * Microsoft Windows Defender x64 Edition
- * Microsoft Windows Defender in Windows Vista
- * Microsoft Forefront Security for Exchange Server
- * Microsoft Forefront Security for SharePoint

[NT] Vulnerability in Microsoft Malware Protection Engine Allows Code Execution (MS07-010)

Affected Components:

- * Microsoft Malware Protection Engine

Mitigating Factors for Microsoft Malware Protection Engine Vulnerability – CVE-2006-5270:

- * We have not identified any mitigating factors for this vulnerability.

Workarounds for Microsoft Malware Protection Engine Vulnerability – CVE-2006-5270:

* Microsoft Forefront Security for Exchange Server, Microsoft Forefront Security for SharePoint, and Microsoft Antigen supports multiple engines in addition to the Microsoft Malware Protection Engine on a single system. If multiple engines are available on an affected system, administrators can disable the Microsoft Malware Protection Engine as a workaround, until the Microsoft Malware Protection Engine can be updated. Before disabling the Microsoft Malware Protection Engine, administrators should ensure they have installed the latest virus signatures for any third party engine.

- * We have not identified any workarounds for Windows Live OneCare and Microsoft Windows Defender.

FAQ for Microsoft Malware Protection Engine Vulnerability – CVE-2006-5270:

What is the scope of the vulnerability?

A remote code execution vulnerability exists in the Microsoft Malware Protection Engine because of the way that it parses Portable Document Format (PDF) files. An attacker could exploit the vulnerability by constructing a specially crafted PDF file that could potentially allow remote code execution when the target computer system receives, and the Microsoft Malware Protection Engine scans, the PDF file.

What causes the vulnerability?

An integer overflow in the Microsoft Malware Protection Engine when processing a specially crafted PDF file.

What is the Microsoft Malware Protection Engine?

The Microsoft Malware Protection Engine, `mpengine.dll`, provides the scanning, detection and cleaning capabilities for the following antivirus and antispyware clients: Windows Live OneCare, Microsoft Forefront Security, Microsoft Antigen, and Windows Defender.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could cause remote code execution and take complete control of the affected system.

Who could exploit the vulnerability?

Any anonymous user who could deliver a specially crafted PDF to an affected system could try to exploit this vulnerability.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a specially

[NT] Vulnerability in Microsoft Malware Protection Engine Allows Code Execution (MS07-010)

crafted PDF attachment and forcing an affected system to process the PDF. When Microsoft Malware Protection Engine on the target machine automatically scans the PDF, the PDF could then cause the affected system to execute arbitrary code.

Finally, an attacker could also make a specially crafted PDF available on a Web site. An attacker would have no way to force users to visit a particular Web site. Instead, an attacker would have to convince them to visit the Web site, typically by getting them to click a link that takes them to the attacker's site.

What systems are primarily at risk from the vulnerability?

Any Microsoft Antivirus client that uses the Microsoft Malware Protection Engine and whose filters are configured to allow PDF file processing is at risk.

What does the update do?

The update removes the integer overflow vulnerability by modifying the way that the Microsoft Malware Protection Engine validates the length of data in the PDF before passing the data to the allocated buffer.

When this security bulletin was issued, had this vulnerability been publicly disclosed?

No. Microsoft received information about this vulnerability through responsible disclosure. Microsoft had not received any information to indicate that this vulnerability had been publicly disclosed when this security bulletin was originally issued. This security bulletin addresses the vulnerability as well as additional issues discovered through internal investigations.

When this security bulletin was issued, had Microsoft received any reports that this vulnerability was being exploited?

No. Microsoft had not received any information to indicate that this vulnerability had been publicly used to attack customers and had not seen any examples of proof of concept code published when this security bulletin was originally issued.

ADDITIONAL INFORMATION

The information has been provided by Microsoft Security Bulletin MS07-010.

The original article can be found at:

<http://www.microsoft.com/technet/security/bulletin/ms07-010.msp>

<http://www.microsoft.com/technet/security/bulletin/ms07-010.msp>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

[NT] Vulnerability in Microsoft Malware Protection Engine Allows Code Execution (MS07-010)

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.