

# [NT] Vulnerability in Pragmatic General Multicast (PGM) Allows Code Execution (MS06-052)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-09/msg00010.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 13 Sep 2006 08:50:43 +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 Pragmatic General Multicast (PGM) Allows Code Execution (MS06-052)

---

## SUMMARY

There is a remote code execution vulnerability that could allow an attacker to send a specially crafted multicast message to an affected system and execute code on the affected system. The MSMQ service, which is the Windows service needed to allow PGM communications is not installed by default.

## DETAILS

### Affected Software:

\* Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=ce264ac4-6ca3-4732-9016-3143ff1bca2f>>

Download the update

### Non-Affected Software:

\* Microsoft Windows 2000 Service Pack 4

\* Microsoft Windows XP Professional x64 Edition

\* Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service

## [NT] Vulnerability in Pragmatic General Multicast (PGM) Allows Code Execution (MS06-052)

### Pack 1

\* Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows Server 2003 with SP1 for Itanium-based Systems

\* Microsoft Windows Server 2003 x64 Edition

### CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3442>>

CVE-2006-3442

### Mitigating Factors for PGM Code Execution Vulnerability – CVE-2006-3442:

\* For customers who require the affected component, firewall best practices and standard default firewall configurations can help protect networks from attacks that originate outside the enterprise perimeter.

Best practices recommend that systems that are connected to the Internet have a minimal number of ports exposed.

\* Pragmatic General Multicast (PGM) is only supported when Microsoft Message Queuing (MSMQ) 3.0 is installed. The MSMQ service is not installed by default.

### FAQ for PGM Code Execution Vulnerability – CVE-2006-3442:

What is the scope of the vulnerability?

This is a remote code execution vulnerability. An attacker who successfully exploited this vulnerability could remotely 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.

What causes the vulnerability?

Invalid memory access in the Pragmatic General Multicast (PGM) multicast protocol implementation in Windows XP.

What is Pragmatic General Multicast (PGM)?

PGM is a reliable and scalable multicast protocol that enables receivers to detect loss, request retransmission of lost data, or notify an application of unrecoverable loss. PGM is a receiver-reliable protocol, which means the receiver is responsible for ensuring all data is received, absolving the sender of reception responsibility. PGM is appropriate for applications that require duplicate-free multicast data delivery from multiple sources to multiple receivers. PGM does not support acknowledged delivery, nor does it guarantee ordering of packets from multiple senders. For more information on PGM please see the following MSDN Article.

What is MSMQ and the MSMQ Service?

Microsoft Message Queuing Services (MSMQ) enables applications running at different times to communicate across heterogeneous networks and systems that may be temporarily offline. For more information on PGM please see the following MSDN Article.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could take

## [NT] Vulnerability in Pragmatic General Multicast (PGM) Allows Code Execution (MS06–052)

complete control of the affected system.

Who could exploit the vulnerability?

On Windows XP, any anonymous user who could deliver a specially crafted message to the affected system could try to exploit this vulnerability.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by sending a specially crafted message that could communicate with a vulnerable system through MSMQ.

What systems are primarily at risk from the vulnerability?

Windows XP systems that have installed the MSMQ service are primarily at risk from this vulnerability. The service is not installed by default.

Note Windows XP Professional x64 Edition shares its implementation of MSMQ with Windows Server 2003 x64 Edition and is therefore not affected by this vulnerability.

Could the vulnerability be exploited over the Internet?

Yes. An attacker could try to exploit this vulnerability over the Internet. Firewall best practices and standard default firewall configurations can help protect against attacks that originate from the Internet. Microsoft has provided information about how you can help protect your PC. End users can visit the Protect Your PC Web site. IT professionals can visit the Security Guidance Center Web site.

What does the update do?

The update removes the vulnerability by modifying the way that a PGM message is validated before it passes the message 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.

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 David Warden of NuPaper Inc.

The original article can be found at:

<<http://www.microsoft.com/technet/security/bulletin/ms06-052.mspx>>  
<http://www.microsoft.com/technet/security/bulletin/ms06-052.mspx>

=====

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@xxxxxxxxxxxxxxxxx

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

=====

=====

**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.