



**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory**

February 13, 2007

The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

STATE OF ALASKA ADVISORY NUMBER:

2007-05

DATE ISSUED:

02/13/2007

SUBJECT:

Vulnerability in Microsoft Malware Protection Engine Could Allow Remote Code Execution

OVERVIEW:

Microsoft is reporting a new vulnerability in the way several Microsoft antivirus and security products process Adobe Portable Document Format (PDF) files. Of particular concern is Microsoft's antivirus email gateway product, Antigen, which is used by organizations to identify and quarantine malicious code. If an exploit is successful, an attacker could obtain complete control of this critical system.

SYSTEMS AFFECTED:

- 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

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: **High**

DESCRIPTION:

Microsoft security bulletin MS07-010 (CVE-2006-5270) reports a new vulnerability found in the way Microsoft Malware Protection Engine parses PDF files. The Malware Protection Engine provides the scanning, detection and cleaning capabilities for various Microsoft antivirus and antispymware clients. When the Microsoft Malware Protection Engine receives and scans a specially crafted PDF file, it could allow for remote code execution that can give an attacker complete control of the affected system. User interaction is not required in order to this vulnerability to be exploited.

Please note that this engine is used by Microsoft Antigen for Exchange Server 9.x, and Microsoft Antigen for SMTP Gateway 9.x.

RECOMMENDATIONS:

We recommend that the following action be taken:

- Apply all the appropriate patches provided by Microsoft to vulnerable systems as soon as possible after appropriate testing. A listing of the patches for this vulnerability is located at:
<http://www.microsoft.com/technet/security/Bulletin/MS07-010.mspx> .
Although desktops, laptops and servers are all affected, organizations are encouraged to prioritize patching their Antigen servers first.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/Bulletin/MS07-010.mspx>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5270>