



Australian Government

Attorney-General's Department



AUSTRALIA'S NATIONAL
COMPUTER EMERGENCY RESPONSE TEAM

CERT Australia Industry News

Vulnerability Discovered in Windows Graphics Rendering Engine

Summary

A vulnerability has been identified in the Windows Graphics Rendering Engine in Windows Vista, Windows Server 2008, Windows Server 2003 and Windows XP. If successfully exploited the vulnerability may allow an attacker to execute arbitrary code with the permissions of the currently logged in user. At the time of writing no official patch was available.

Technical Details

A vulnerability in the Windows Graphics Rendering Engine in older versions of Microsoft Windows has been found that may allow an attacker to execute arbitrary code with the permissions of the currently logged in user.

Windows 7 and Windows Server 2008 R2 are not affected.

In order to exploit this vulnerability, an attacker would have to convince the user to go to a malicious website or open a malicious Word or PowerPoint file.

At the time of writing no patch was available, however Microsoft is investigating and a temporary workaround is available in their advisory. [1]

Exploit code has been made public.

CVE-2010-3970 has been assigned to this vulnerability. [2]

Business Impact

While the impact of vulnerabilities on individual businesses varies, an attacker could use this vulnerability to compromise confidential data or run commands (including the installation of malicious programs) if a vulnerable computer is used to access a malicious site or file. An attacker could then launch attacks on internal systems from such a compromised computer, leading to further damage.

For more information regarding mitigations, please refer to the "Additional Information" section below.

Additional Information

[1] <http://www.microsoft.com/technet/security/advisory/2490606.msp>

[2] <http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3970>

This document remains the property of the Australian Government. The information contained in this document is for the use of the intended recipient only and may contain confidential or privileged information. If this document has been received in error, that error does not constitute a waiver of any confidentiality, privilege or copyright in respect of this document or the information it contains.

The material and information in this document is general information only and is not intended to be advice. The material and information is not adapted to any particular person's circumstances and therefore cannot be relied upon to be of assistance in any particular case. You should base any action you take exclusively on your own methodologies, assessments and judgement, after seeking specific advice from such relevant experts and advisers as you consider necessary or desirable. To the extent permitted by law, the Australian Government has no liability to you in respect of damage that you might suffer that is directly or indirectly related to this document, no matter how arising (including as a result of negligence).