

US-CERT Technical Cyber Security Alert TA06-283A -- Microsoft Updates for Vulnerabilities in Windows, Office, and Internet Explorer

Source: <http://www.derkeiler.com/Mailing-Lists/Cert/2006-10/msg00001.html>

- *From:* CERT Advisory <cert-advisory@xxxxxxxx>
 - *Date:* Tue, 10 Oct 2006 15:31:47 -0400
-

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

National Cyber Alert System

Technical Cyber Security Alert TA06-283A

Microsoft Updates for Vulnerabilities in Windows, Office, and Internet Explorer

Original release date: October 10, 2006

Last revised: --

Source: US-CERT

Systems Affected

- * Microsoft Windows
- * Microsoft Office
- * Microsoft Internet Explorer

Overview

Microsoft has released updates that address critical vulnerabilities in Microsoft Windows, Internet Explorer, and Microsoft Office. Exploitation of these vulnerabilities could allow a remote, unauthenticated attacker to execute arbitrary code or cause a denial of service on a vulnerable system.

I. Description

Microsoft has released updates to address vulnerabilities in Microsoft Windows, Internet Explorer, and Microsoft Office as part of the Microsoft Security Bulletin Summary for October 2006. The summary lists ten Microsoft Security Bulletins. Two of the Bulletins discuss previously disclosed vulnerabilities that are actively being exploited:

Microsoft Security Bulletin MS06-057 addresses a remote code execution vulnerability in the WebFolderIcon ActiveX control. More information is available in VU#753044.

Microsoft Security Bulletin MS06-058 addresses a remote code execution vulnerability in Microsoft PowerPoint. More information is available in VU#231204.

Further information on vulnerabilities addressed by the October 2006 Security Bulletins will be available in Vulnerability Notes.

Microsoft has announced the end of support for Windows XP Service Pack

1. According to Microsoft:

On October 10, 2006, Microsoft will end all public assisted support for Windows XP Service Pack 1 (SP1). After this date, Microsoft will no longer provide any incident support options or security updates for this retired service pack under the policies defined by the Microsoft Support Lifecycle policy.

We strongly encourage Windows XP users to upgrade to Windows XP Service Pack 2 (SP2) as soon as possible.

II. Impact

A remote, unauthenticated attacker could execute arbitrary code on a vulnerable system. An attacker may also be able to cause a denial of service.

III. Solution

Apply updates from Microsoft

Microsoft has provided updates for these vulnerabilities in the October 2006 Security Bulletins. The Security Bulletins describe any known issues related to the updates. Note any known issues described in the Bulletins and test for any potentially adverse affects in your environment.

Updates for Microsoft Windows and Microsoft Office XP and later are

available on the Microsoft Update site. Microsoft Office 2000 updates are available on the Microsoft Office Update site.

System administrators may wish to consider using Windows Server Update Services (WSUS).

References

- * US-CERT Vulnerability Notes for Microsoft October 2006 updates – <http://www.kb.cert.org/vuls/byid?searchview&query=ms06-oct>
- * Securing Your Web Browser – http://www.us-cert.gov/reading_room/securing_browser/
- * Microsoft Security Bulletin Summary for October 2006 – <http://www.microsoft.com/technet/security/bulletin/ms06-oct.mspx>
- * Microsoft Update – <https://update.microsoft.com/microsoftupdate/>
- * Microsoft Office Update – <http://officeupdate.microsoft.com/>
- * End of support for Windows 98, Windows Me, and Windows XP Service Pack 1 – <http://www.microsoft.com/windows/support/endofsupport.mspx#EHB>
- * Windows Server Update Services – <http://www.microsoft.com/windowssserversystem/updateservices/default.mspx>

The most recent version of this document can be found at:

<http://www.us-cert.gov/cas/techalerts/TA06-283A.html>

Feedback can be directed to US-CERT Technical Staff. Please send email to cert@xxxxxxxx with "TA06-283A Feedback VU#703936" in the subject.

Produced 2006 by US-CERT, a government organization.

Terms of use:

<http://www.us-cert.gov/legal.html>

Revision History

October 10, 2006: Initial release

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.2.1 (GNU/Linux)

iQEVAwUBRSvzt+xOF3G+ig+rAQJmAggAkNBW57N0Ob9Mvelr+ByiV4PZUGkoibd1
6wB7wTYSD4C2YhlQGlbgaEk5H2ZahC6Q+s18BuEtPwuxOHqbws/ycaiAoeiH+J0m
xIXKpzC17pzcnk9qfPBmjNrsdFuzbcL1N4712VAKLoVnlMj1IH+NHJMBVMbtLSrZ
OD7PxlmAoaALsnapRySgJJAb06oPwBSPdOEazIofWL48bz1JFLwOSHn4EtTbqD7K
8AGbWGix7RloRx6Q39Th3DdRPEy3xEM5q5dIAIKaF5s21HT5p5PPH+VYmZE6l9e3
RZ7FUIqZBucFFHW/XQFvEveoGjrX2Vng+qerUHy76uU37wzG49urXQ==
=8Gam

-----END PGP SIGNATURE-----