

US-CERT – Microsoft Updates for Multiple Vulnerabilities

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2007-07/msg00051.html>

- *From:* cbgerry <cbgerry@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 10 Jul 2007 17:23:54 -0700
-

US-CERT Technical Cyber Security Alert TA07-191A -- Microsoft Updates for Multiple Vulnerabilities

Posted: Tue Jul 10, 2007 6:44 pm Post subject: US-CERT – Microsoft Updates for Multiple Vulnerabilities

US-CERT Technical Cyber Security Alert TA07-191A -- Microsoft Updates for Multiple Vulnerabilities

----- Original Message -----

From: US-CERT Technical Alerts
To: technical-alerts@xxxxxxxxxxxx
Sent: Tuesday, July 10, 2007 4:52 PM
Subject: US-CERT Technical Cyber Security Alert TA07-191A -- Microsoft Updates for Multiple Vulnerabilities

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

Hash: SHA1

National Cyber Alert System

Technical Cyber Security Alert TA07-191A

Microsoft Updates for Multiple Vulnerabilities

Original release date: July 10, 2007

Last revised: --

Source: US-CERT

Systems Affected

US-CERT – Microsoft Updates for Multiple Vulnerabilities

- * Microsoft Windows
- * Microsoft Excel
- * Microsoft Publisher
- * Microsoft .NET Framework
- * Microsoft Internet Information Services (IIS)
- * Microsoft Windows Vista Firewall

Overview

Microsoft has released updates that address critical vulnerabilities in Microsoft Windows, Excel, Publisher, .NET Framework, Internet Information Services, and Windows Vista Firewall. 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 that affect Microsoft Windows, Excel, Publisher, .NET Framework, Internet Information Services, and Windows Vista Firewall as part of the Microsoft Security Bulletin Summary for July 2007. The most severe vulnerabilities could allow a remote, unauthenticated attacker to execute arbitrary code or cause a denial of service on a vulnerable system.

Further information about the vulnerabilities addressed by these updates is available in the Vulnerability Notes Database

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 July 2007 Security Bulletins. The Security Bulletins describe any known issues related to the updates. Administrators are encouraged to note any known issues that are described in the Bulletins and test for any potentially adverse effects.

System administrators may wish to consider using an automated patch

US-CERT – Microsoft Updates for Multiple Vulnerabilities

distribution system such as Windows Server Update Services (WSUS).

IV. References

* US-CERT Vulnerability Notes for Microsoft July 2007 updates –
<<http://www.kb.cert.org/vuls/byid?searchview&query=ms07-jul>>

* Securing Your Web Browser –
<http://www.us-cert.gov/reading_room/securing_browser/>

* Microsoft Security Bulletin Summary for July 2007 –
<<http://www.microsoft.com/technet/security/bulletin/ms07-jul.mspx>>

* Microsoft Update – <<https://update.microsoft.com/microsoftupdate/>>

* Microsoft Office Update – <<http://officeupdate.microsoft.com/>>

* Windows Server Update Services –
<<http://www.microsoft.com/windowsserversystem/updateservices/default.mspx>>

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

<<http://www.us-cert.gov/cas/techalerts/TA07-191A.html>>

Feedback can be directed to US-CERT Technical Staff. Please send email to <cert@xxxxxxxx> with "TA07-191A Feedback VU#487905" in the subject.

For instructions on subscribing to or unsubscribing from this mailing list, visit <<http://www.us-cert.gov/cas/signup.html>>.

Produced 2007 by US-CERT, a government organization.

Terms of use:

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

Revision History

July 10, 2007: Initial release

US-CERT – Microsoft Updates for Multiple Vulnerabilities

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

Version: GnuPG v1.2.1 (GNU/Linux)

iQEVAwUBRpPwhvRFkHkM87XOAQKWiQf/XFpYurcCFZ1qG700NatqdY7wL6pO4qbv
hGzdzUJH+aRN7b6XaEE/ZLprWnyj2H8HbH+HAHOuKDOxBI7N6PQ4WPaeZ14tDsNP
pNFg81LjE5Hlj6h5N2p8XML3t/4X7a7wk5YB7nhiBdisxAJ7iNjQ1BawjTIA9/kl
dTaiRW2njHpupGLWuin60U/di12ji3JirgJHfiRK6Ruiqnv56rM7LS9IOT1HV5RR
0otlr1Dttndmgveb0YOiz7A36nwMiCEUzcUu2rKzARpZ4gMBIrSbfkAJpyUE0w3K
WMh1tgEt3fooTgvBUhpDjfbMNka85wGbpizcsKnw6VVzIQAlr0y3Q==
=FRhW

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

TOPIC# <http://bluecollarpc.net/phpbb2/viewtopic.php?p=740#740>

*****Forum Moderator *****

BlueCollarPC.Net Forums Spyware Removal and Computing Safety

<http://bluecollarpc.net/phpbb2/index.php>