

US-CERT Technical Cyber Security Alert TA07-317A -- Microsoft Updates for Multiple Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Cert/2007-11/msg00001.html>

- *From:* CERT Advisory <cert-advisory@xxxxxxxx>
 - *Date:* Tue, 13 Nov 2007 14:53:46 -0500
-

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

Hash: SHA1

National Cyber Alert System

Technical Cyber Security Alert TA07-317A

Microsoft Updates for Multiple Vulnerabilities

Original release date: November 13, 2007

Last revised: --

Source: US-CERT

Systems Affected

- * Microsoft Windows
- * Microsoft Windows DNS Server

Overview

Microsoft has released updates that address critical vulnerabilities in Microsoft Windows and Microsoft Windows DNS Server. Exploitation of these vulnerabilities could allow a remote, unauthenticated attacker to execute arbitrary commands or to cause a Windows DNS server to provide incorrect DNS responses.

I. Description

Microsoft has released updates to address vulnerabilities that affect Microsoft Windows and Microsoft Windows DNS Server as part of the Microsoft Security Bulletin Summary for November 2007. The most severe

US-CERT Technical Cyber Security Alert TA07-317A -- Microsoft Updates for Multiple Vulnerabilities

vulnerabilities could allow a remote, unauthenticated attacker to execute arbitrary commands or cause a Windows DNS server to provide incorrect DNS responses.

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 commands on a vulnerable system. An attacker may also be able to cause a Windows DNS server to provide incorrect responses to DNS queries.

III. Solution

Apply updates from Microsoft

Microsoft has provided updates for these vulnerabilities in the November 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 should consider using an automated patch distribution system such as Windows Server Update Services (WSUS).

IV. References

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

* Microsoft Security Bulletin Summary for November 2007 –
<<http://www.microsoft.com/technet/security/bulletin/ms07-nov.msp>>

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

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

* Securing Your Web Browser –
<http://www.cert.org/tech_tips/securing_browser/>

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

<<http://www.us-cert.gov/cas/techalerts/TA07-317A.html>>

Feedback can be directed to US-CERT Technical Staff. Please send email to <cert@xxxxxxx> with "TA07-317A Feedback VU#484649" 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

November 13, 2007: Initial release

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

Version: GnuPG v1.2.1 (GNU/Linux)

iQEVAwUBRzn+L/RfKHkM87XOAQIP7wgAmXsO3NefxyFn/eFlLvWeGpVNLUQKdso
VuU2/ktEtMNKQeFgsoZnFMHuKWp2hIMXZPCrelegVHszYHwSmE92QsHvumxVg863
iP3e4wXoL5uYpoYXJuZR18Ee65GdRlsZBp2HS5bqDm2yWAdKLyEfyVArkmvjJFkM
LydRRMVYnyl4aLBGDh/xzowu6jtKmdMRtFQYDac6A/INdJpAm6lo8OKPG2mY80vh
8acL6ObfFT45UpYkxCFaCvRMn4/Ts24j3cpnQxmNE9/veENVJxumT6sUH56rrkw/
vLZIK1QMwGPXOXOg9rc7UktWqc9iYFsHmTVC8kwB8ksfk26drpmu1w==
=24yY

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