SÛNNET BESKERMING

-

Microsoft Security Patch Brief

September 2006

Sûnnet Beskerming Pty. Ltd.

ABN 17 108 355 540
info@beskerming.com
http://www.beskerming.com

Revised - September 2006

Introduction

Microsoft has released five patches with their September Security Update. Three of the patches were as described in the advanced notification, and two have been re-released from August. The two re-released patches are rated critical, along with one of the new patches, and the remaining two patches are rated as Important and Moderate. All patches should be applied as soon as possible to mitigate against known exploits.

MS06-040 (Critical) – Re-Release

Vulnerable Products

Microsoft Windows 2000
Microsoft Windows XP
Microsoft Windows 2003

Vulnerability

MS06-040 provides fixes for a vulnerability within the 'Server Service' in the affected versions of Windows. This vulnerability can allow a remote attacker to take complete control of a vulnerable system, and affects all systems by default.

Mitigation

If the patch can not be immediately applied, use of IPSec and TCP/IP filtering can help manage the risk that an unpatched system faces. Blocking TCP ports 139 and 445 at perimeter firewalls and on individual systems (host-based) can prevent spread of automated attacks against this issue.

Known Issues

By not patching, some of the mitigation steps (blocking 139 and 445 from all systems) can have a serious negative effect on system functionality. Numerous sample exploits are available, and this vulnerability is being actively attacked and exploited by a number of network worms. This re-released version is the updated patch that was issued in late August, following system instability issues on systems where applications routinely used large sections of contiguous memory.

Download

http://www.microsoft.com/technet/security/Bulletin/MS06-040.mspx

info@beskerming.com
http://www.beskerming.com

MS06-042 (Critical) – Re-Release

Vulnerable Products

Microsoft Internet Explorer

Vulnerability

MS06-042 is the latest cumulative update for Internet Explorer, providing patches for several critical vulnerabilities, the oldest of which is from December 2004. These vulnerabilities affect FTP, HTML rendering, CSS support, and various scripting support, with most leading to arbitrary code execution opportunities for a remote attacker. This update also replaces MS06-021.

Mitigation

Due to the extent and seriousness of the vulnerabilities patched through this update, the only mitigation that is recommended is the use of an alternate (and current) web browser until the patch can be applied.

Known Issues

Exploit code has been available for the FTP command injection flaw since December 2004, and it can be rapidly developed into an attack that can be implemented through relatively innocent-looking website code (or even advertising banner code). If a replacement browser is used in the interim, it may cause accessibility issues for sites that rely upon ActiveX components for full user functionality. When originally issued, the patch introduced a remote code execution bug (long URL), which has been addressed with this re-release.

Download

http://www.microsoft.com/technet/security/Bulletin/MS06-042.mspx

info@beskerming.com
http://www.beskerming.com

MS06-052 (Important)

Vulnerable Products

Microsoft Windows 2000
Microsoft Windows XP
Microsoft Windows 2003

Vulnerability

MS06-052 fixes an issue with the implementation of multicast messaging. Microsoft have advised that it is possible to take control of a vulnerable system by sending a malicious PGM packet across the network. Fortunately the affected service is not installed by default. Users who have needed to install MSMQ are advised that this patch is Critical for them.

Mitigation

There is no non-patch mitigation that is recommended, other than not installing MSMQ 3.0 on systems that do not require it (MSMQ is not installed by default).

Known Issues

Due to the apparent ease of exploitation, users who are unable to apply the patch are recommended to adjust their perimeter defences, in order to block against attacks coming from across the Internet.

Download

http://www.microsoft.com/technet/security/Bulletin/MS06-052.mspx

MS06-053 (Moderate)

Vulnerable Products

Microsoft Windows 2000
Microsoft Windows XP
Microsoft Windows 2003

Vulnerability

MS06-053 patches an issue with the Indexing Service, which can allow a remote attacker to run scripts in the context of the current user. The issue is due to poor query handling in the service. Although minor victim interaction is required, successful exploitation of this issue can be partially automated. This patch also replaces MS05-003.

Mitigation

Several mitigation techniques have been suggested by Microsoft. The first is not to surf the Internet while the current system is being used for any sort of server role. Secondly, it is possible to disable page encoding auto-detection in Internet Explorer (via View->Encoding). Thirdly, Windows 2000 (IIS 5.0) users can install URLScan (from Microsoft) to prevent exploitation. Finally, it is possible to disable / remove the ISAPI Indexing Service extension / Indexing Service extension from systems where it is not required.

Known Issues

Disabling page encoding in Internet Explorer may cause improper display of web pages. Using URLScan will stop display of .IDA, .IDQ, and .HTW content. Disablement or removal of the service from systems can cause problems in applications that rely upon the service for functionality, and should only be attempted by administrators who are confident that system instability will not result (or who can easily restore their systems).

Download

http://www.microsoft.com/technet/security/Bulletin/MS06-053.mspx

MS06-054 (Critical)

Vulnerable Products

Microsoft Office 2000
Microsoft Office XP (2002)
Microsoft Office 2003

Vulnerability

MS06-054 fixes a remote code execution vulnerability with Publisher (installed with the Professional versions of Office). The specific issue is a buffer overflow due to an unchecked string that is passed to the vulnerable buffer.

Mitigation

The only recommended mitigation from Microsoft is to not open Publisher files from untrusted sources.

Known Issues

Following the patch installation, Publisher 2000 and 2002 users will no longer be able to interact with Publisher 2.0 files. Opening a malicious file following patch application may cause Publisher to crash (but not allow code execution).

Download

http://www.microsoft.com/technet/security/Bulletin/MS06-054.mspx

info@beskerming.com
http://www.beskerming.com

About us:

Sûnnet Beskerming is an Innovative Information Security company based in Adelaide's northern suburbs. Delivering rapid, accurate security advice and assessment, Sûnnet Beskerming is one of the leading Information Security reporting companies globally.

For more information or help with the above advisories or other security advice, please don't hesitate to contact us at:

info@beskerming.com
http://www.beskerming.com
Tel: +61 (0) 410 707 444

FREE Advisory mailing list –
http://www.skiifwrald.com/mailman/listinfo/alertmailinglist_skiifwrald.com