

# Sistem güvenliği

Yama yönetimi ile başladığımız yazımızı bu ay güvenlik araçları ile sona erdiriyoruz.

**B**u ay geçen yazımızda değindiğimiz güvenlik araçlarına, hem de değinmediğimiz ancak Microsoft tarafından önerilen bazı güvenlik araçlarına göz atarak ne tür araçların ne tür faydalar sağlayabileceğini beraberce görmeye çalışacağız.

## Microsoft Baseline Security Analyzer (MBSA)

**İndirilecek adres:** <http://download.microsoft.com/download/8/e/e/8ee73487-4d56-4f7f-92f2-2bdc5c5385b3/mbsase-tup.msi>

**Boyutu:** 5.68 MB

**Kurulumun desteklediği sistemler:** İşletim sistemi olarak Windows Server 2005, Windows 2000 ve Windows XP üzerine kurulabilmekte. Ayrıca bu işletim sistemlerinde Internet Explorer 5.01 veya daha üstündeki bir sürüm bulunması öneriliyor. Buna ek olarak MSXML 3.0 SP2 veya daha üstünde XML Parser'ın sistemde yüklü olması bekleniyor. Bu uygulamayı da <http://msdn.microsoft.com/library/default.asp?url=/downloads/list/xmlgeneral.asp> adresinden indirebilirsiniz.

Son olarak kurulacak makinede MBSA kullanılabilmesi için Workstation servisinin ve server servisinin çalışır durumda olması gerekmektedir. Eğer kendi makinanızda değil de ağda arama yapacaksanız kurulacak makinede bir de Client for Microsoft Networks servisinin çalışır olması şart.

### Tarama yapılacak makinede taranabilen uygulamalar:

- Windows NT 4.0 SP4 veya yukarısı
- Windows 2000
- Windows XP
- Windows Server 2005
- IE 5.01 veya üstü
- IIS 4.0 ve IIS 5.0 (IIS vulnerability taraması için)
- SQL 7.0 ve SQL 2000 (SQL vulnerability taraması için)
- Microsoft Office 2000 ve XP (Desktop Application vulnerability taraması için)

Bunlara ek olarak uzaktan tarama yapılabilmesi için tarama yapılacak makinenin üzerinde sunucu servisinin, remote registry servisinin çalışması gerekmektedir. Tabii o makinede local admin hakkına sahip olmamız da şart.

Kısacası, bu güvenlik aracı bize ister tek bir makinede istersek de belli bir IP aralığı vererek tüm makinelerde ne gibi açıklar var, hangi güvenlik yamaları eksik ve ne gibi işlemler yaparsak daha güvenli hale getirebiliriz; bunların yollarını göstermekte. Uyarı verdiği noktalarda

### CIHAN BAYKAL

(cihanb@winnetmag.com.tr) Chip Türkiye ve Windows & .Net Magazine'e katkıda bulunan yazarlardandır. Özel bir firmada Kurumsal Destek Mühendisi olarak görev yapmaktadır. MCSE, MCP+I sertifikalarına sahiptir.



**Şekil 8:** MBSA rapor sonucu.

bize yol göstermesi ve çözümler üretmesi, bu aracın en güzel özelliklerinden birisi. Raporun okunabilirliği de kullanıcılar için büyük rahatlık sağlayacaktır.

## Software Update Services (SUS)

**İndirilecek adres:** <http://download.microsoft.com/download/0/b/9/0b97f864-2408-4748-ad963691e2451006/SUS10SP1.exe>

**Boyutu:** 33009 KB

### Sistem gereksinimleri:

Windows 2000 ve Windows Server 2003

6 GB sabit disk alanı  
512 MB Ram  
Pentium III 700 Mhz. CPU

Şubat ayında yazdığımız Software Update Services yazısı sonrası çıkan SUS SP1 ile her şey daha da kolaylaşmış durumda. Örneğin daha önce Windows 2000 Domain Controller üzerinde ve Small Business Server üzerinde SUS kurulamazken artık bu sistemlerin üzerlerine de SUS Server kurulabilmekte. Buna ek olarak Windows 2005 desteği ve artık Service Pack deployment'ı da desteklediğinden, inanılmaz fayda sağlayacağını düşündüğümüz bir uygulama halini almış gibi gözükmemekte.

**Kısaca SUS'u tanıyalım ve nasıl çalıştığını biraz açıklamaya çalışalım.**

SUS uygulamasını internetten Windows 2000 veya Windows Server 2003 makinesine kurduğunuzda, IIS üzerine yerlesen bileşenleri ile servis vermeye başlamakta. Daha önceki adımlarda bahsettiğimiz gibi, sistemlerinize bir yama veya bir güncelleme geçmeden önce bir zarar verebilme ihtimaline karşı (bu zarar verme, uyumsuzluk veya yanlış bir seçim olabilir) test ortamında denemelerinizi yapıp sonuçlarını gördükten sonra gerçek ortama geçme önerisinden bah-

setmiştik. SUS'ta ise bunu sağlayabilecek bir özellik mevcut. Kurulum bittikten sonra Synchronize Server diyerek istemiş olduğunuz İşletim Sistemleri için varolan tüm yamaları Windows Update'ten kendi veritabanına indirmektedir. Bu işlem sonrası ise sizden tüm bu yamalar için tek tek onaylamanız bekleniyor. Aksi takdirde hiçbir makine bu SUS Server'dan güncelleme ve yamaları çekemiyor.

Siz testlerinizi bitirip onaylarınızı verdikten sonra, daha önceden tüm makinelerinizin kurmuş olduğunuz SUS Server'dan güncellemeleri çekmesini sağladığımız için (bu işlemi group policy veya elle client registry'den yapılabiliyorsunuz, tüm ayrıntılar deployment guide'da mevcut) makineler periyodik zamanlarda SUS Server ile konuşarak herhangi bir güncelleme varsa çekip sistemlerine kuracaklardır. Bu sayede ağ üzerindeki tüm makinelere tek bir yerden güncelleme yapmanız mümkün olmaktadır.

Bu konunun bir güzel tarafı daha mevcut. Örneğin dilediğinizce Windows Update sayfasına girip güncelleme yapmasını önlemek ve tamamen sizin kontrolünüzde olmasını sağlamak isteyebilirsiniz. Bunu da kullandığımız firewall'dan Windows Update sayfasını

engelleyerek tüm istemcilerde de SUS Server'ı referans göstererek yapmanız çok basit.

### KB 824146 Scanning Tool

Bildiğiniz gibi, geçtiğimiz dönemde bir hayli baş ağrıtan ve hala tehlikesi devam eden MSBLASTER virüsü, RPC üzerindeki bir açıktan faydalanıp buffer overrun yaratarak sistemlere zarar veriyordu. Microsoft, bu konuda son çıkardığı MS-039 yaması ile açığı kapattı ve tüm bilgisayarlara tüm Microsoft işletim sistemlerine kesinlikle ağa ve internete bağlanmadan önce yüklenmesini önerdi.

Yine de virüsün ağızda hangi bilgisayarlarda olduğunu öğrenmenin kolay bir yolu mevcut. Bahsedeceğimiz bu araç ile ağızdaki tüm makineler tarıyor ve son çıkan MS-039 yamasının yüklü olup olmadığı bir rapor halinde size sunuluyor. Tabii ki bu aracın tüm diğer bilgisayarlardan rapor çekebilmesi için domain admin hakkına sahip olmanız gerekmektedir.

**Not** – MS-039 ile ilgili daha ayrıntılı bilgiye şu adresten ulaşabilirsiniz. <http://www.microsoft.com/technet/security/Bulletin/MS05-039.asp>

**İndirilecek adres:** <http://support.microsoft.com/default.aspx?scid=kb;en-us;827363>

**Boyutu:** 204 KB

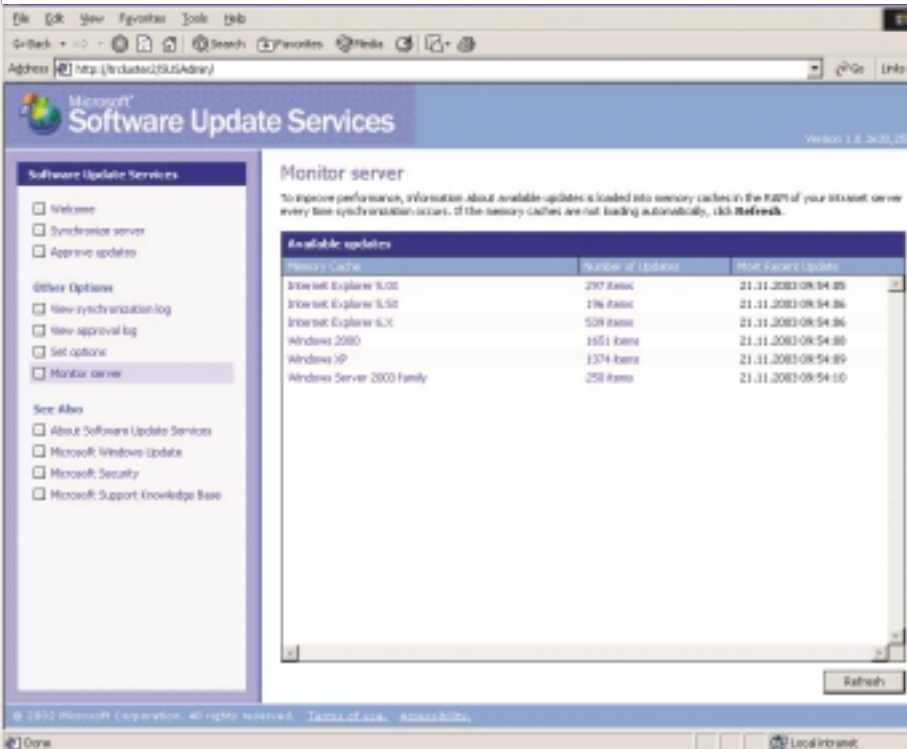
### GCHAIN

Birçok kritik güncelleme, kurulum sonrası makinenin yeniden başlamasını istemektedir. Eğer sistemde bu şekilde birden çok yama yükleyecekseniz, her birini yükleyip makinenin yeniden başlatılmasını beklemek bir hayli zaman alacaktır.

Ayrıca bu türde birkaç adet yamadan oluşacak bir deployment paket hazırlayacaksanız da her yeniden başlatmayı planlamanız ve paketi buna göre tasarlamanız gerekecektir.

İşte, aşağıda verdiğimiz linkte anlatılan yöntemlerle her bir yama için yeniden yüklemeye gerek kalmadan, tüm yamalar için tek bir yeniden başlatma ile kurulumu tamamlayabileceksiniz. Bu sayede zaman kaybı ve paket hazırlığı sırasında ek planlamalar da gerekmeyecek.

**Adres:** <http://support.microsoft.com/default.aspx?scid=KB;EN-US;296861>



Şekil 3: SUS Server yönetim ekranı.

### EventCombMT

Ağda bulunan makinelerin event log'larını incelemek ve yüklemiş olduğunuz kritik güncellemeler sonrası herhangi bir hata oluşup oluşmadığına uzaktan bakmak isteyebilirsiniz.

Bunun için aslında Microsoft Operations Management uygulaması (MOM) önerilmekte.

Ancak ücretsiz ve daha kısıtlı bir uygulama olan EventCombMT kullanmanız da mümkün.

**İndirilecek adres:** <http://download.microsoft.com/download/c/e/3/ce3fd5de-ae44-4c10-858c-67df0b06771e/security/cops.exe>

Son olarak, tüm bu uygulamaların neredeyse tamamını içinde barındıran ve daha birçok özelliği beraberinde getiren SMS 2005 uygulamasına daha giriş yapmadık.

Geçtiğimiz aylarda bu konuda dergimizde bir yazı çıkmıştı, ancak biz önümüzdeki aylarda da bu konuyu işleyerek güvenlik konusuna ve yama yönetimi konusuna bu şekilde nokta koymayı hedefliyoruz.

Yazımızı internette yayımlanan checklist'lerin ve security resource'ların adreslerini vererek tamamlıyoruz. Bu adreslerde sistemlerin adım adım nasıl daha güvenli yapılabileceğine dair bilgileri bulabilirsiniz.

### Security Checklist'leri

Windows 2000 Server Baseline Security  
<http://www.microsoft.com/technet/security/chklist/w2ksvrcl.asp>

Internet Information Services 5.0 Baseline Security  
<http://www.microsoft.com/technet/security/chklist/iis5cl.asp>

Internet Information Services 5 Security Checklist  
<http://www.microsoft.com/technet/security/chklist/iis5chk.asp>

Internet Information Services 5 Security Checklist  
<http://www.microsoft.com/technet/security/chklist/iis5chk.asp>

Windows NT 4.0 Server Baseline Security

<http://www.microsoft.com/technet/security/chklist/nt4svrcl.asp>

Windows NT 4.0 Domain Controller Configuration

<http://www.microsoft.com/technet/security/chklist/dcklcl.asp>

Windows NT 4.0 Member Server Configuration

<http://www.microsoft.com/technet/security/chklist/mbrsrvcl.asp>

Internet Information Server 4 Baseline Security Checklist

<http://www.microsoft.com/technet/security/chklist/iis4cl.asp>

Internet Information Server 4.0 Security Checklist

<http://www.microsoft.com/technet/security/chklist/iischk.asp>

Windows NT 4.0 Workstation Baseline Security

<http://www.microsoft.com/technet/security/chklist/nt4wscl.asp>

Windows NT 4.0 Workstation Configuration

<http://www.microsoft.com/technet/security/chklist/wrkstchk.asp>

Windows XP Baseline Security  
<http://www.microsoft.com/technet/security/chklist/xpcl.asp>

Internet Explorer Configuration  
<http://www.microsoft.com/technet/security/chklist/iecl.asp>

Windows 2000 Professional Baseline Security  
<http://www.microsoft.com/technet/security/chklist/w2kprocl.asp>

Windows 2000 Common Criteria Configuration Guide  
<http://www.microsoft.com/technet/treeview/default.asp?url=/techscg/default.asp>

Windows NT 4.0 C2 Configuration  
<http://www.microsoft.com/technet/security/chklist/c2config.asp>

NIST Baseline Security Settings for Windows 2000 Workstations  
<http://www.microsoft.com/technet>

</archive/security/news/lockguide.asp>

### Security Resource Guides

Windows 2000 Server Security Resource Guide

<http://www.microsoft.com/technet/security/chklist/w2ksvrg.asp>

Internet Information Services (IIS) 5.0 Security Resource Guide

<http://www.microsoft.com/technet/security/chklist/iis50srg.asp>

Windows NT 4.0 Server Security Resource Guide

<http://www.microsoft.com/technet/security/chklist/nt4svsrg.asp>

Internet Information Server (IIS) 4.0 Security Resource Guide

<http://www.microsoft.com/technet/security/chklist/iis40srg.asp>

SQL Server 7.0 Server Security Resource Guide

<http://www.microsoft.com/technet/security/chklist/sql7srg.asp>

SQL Server 2000 Security Resource Guide

<http://www.microsoft.com/technet/security/chklist/sql2ksrg.asp>">

Exchange 2000 Server Security Resource Guide

<http://www.microsoft.com/technet/security/chklist/ex2ksrg.asp>

Windows 98, Windows 95, and Windows Me Desktop Security Resource Guide

<http://www.microsoft.com/technet/security/chklist/w9xmesrg.asp>

Windows 2000 Desktop Security Resource Guide

<http://www.microsoft.com/technet/security/chklist/w2kpsrg.asp>

Office Desktop Security Resource Guide

<http://www.microsoft.com/technet/security/chklist/officsrg.asp>">

Windows XP Desktop Security Resource Guide

<http://www.microsoft.com/technet/security/chklist/winxpsrg.asp>

