



# TALİMAT

## YAMA GÜVENLİĞİ

BŞEÜ-BİDB Belge No	BGYS.TLM.08
İlk Yayın Tarihi/Sayısı	03.09.2018
Revizyon Tarihi	18.10.2022
Revizyon No	01
Sayfa No	1/3

### Revizyon İzleme Tablosu

Rev. No	Rev. Tarihi	Açıklama
01	18.10.2022	Referanslar düzenlendi.

## 1. AMAÇ

Kurumumuzda yama güvenliği için gerekli kuralları belirlemektir.

## 2. SORUMLULUKLAR

Bu talimatın uygulanmasından BİDB sorumludur.

## 3. UYGULAMA

### 3.1. Yama Yönetim Süreci

#### 3.1.1. Değerlendirme

WSUS yazılımı, yöneticinin istemciler, güncellemeler ve güncellemelerin kurulum durumu ile ilgili sürekli bilgi almasını sağlayan raporlar sunmaktadır. Bu raporlar WSUS yama yönetim altyapısında gerçekleşen her türlü olaya ait detaylı bilgiler içermektedir. Değerlendirme sürecindeki iş adımları aşağıdaki gibi özetlenmektedir;

- Mevcut varlıkların envanterinin çıkarılması.
- Yeni yazılım güncelleştirmeleri için kaynakların belirlenmesi
- Mevcut yazılım dağıtım altyapısının değerlendirilmesi
- Yama yönetimi etkinliğinin değerlendirilmesi.

#### 3.1.2. Tanımlama

WSUS yazılımı ile hangi tür güncellemelerin Microsoft Update sitesinden indirileceği seçilebilmektedir. Güncellemelerin indirilmesi sonrasında yönetici güncelleme ihtiyacı olan istemci ve sunucuların listesini görebilmektedir. Tanımlama sürecindeki iş adımları aşağıdaki gibi özetlenmektedir;

- Yeni güncelleştirmelerin bulunması
- Güvenilir bir kaynaktan güncelleştirmelerin elde edilmesi
- Güncelleştirmenin normal veya acil bir değiştirme olduğunun belirlenmesi

#### 3.1.3. Test Ve Planlama

Yöneticinin bu süreçteki amaçlarından birisi güncellemeleri çalışan ortamdan farklı ama çalışan ortama benzer bir ortamda test etmektir. Diğer bir amacı güncelleme sürümlerini planlamak, bunları oluşturmak ve güncellemeleri kabul testinden geçirmektir. Bu süreçteki iş adımları aşağıdaki gibi özetlenmektedir;

- Güncelleme dağıtımının gerçekten gerekli olup olmadığını belirlenmesi
- Güncellemenin nasıl çıkarılacağına planlanması ve güncelleme paketinin oluşturulması



# TALİMAT

## YAMA GÜVENLİĞİ

BŞEÜ-BİDB Belge No	BGYS.TLM.08
İlk Yayın Tarihi/Sayısı	03.09.2018
Revizyon Tarihi	18.10.2022
Revizyon No	01
Sayfa No	2/3

- Güncelleştirmenin üretim ortamına benzer bir test ortamında test edilmesi

### 3.1.4. Yükleme

WSUS yöneticilere hangi güncelleştirmelerin hangi gruba yapılacağını seçme imkanı tanımaktadır. Ayrıca WSUS ile güncelleştirmelerin en geç hangi tarihe kadar kurulması gerektiği de belirlenebilmektedir. Bu süreç içindeki iş adımları aşağıdaki gibi özetlenmektedir;

- Dağıtım için hazırlık yapılması
- Hedef bilgisayarlara güncelleştirmenin yüklenmesi
- Dağıtımın ve dağıtım sonrası bilgisayarların durumun kontrol edilmesi

## 3.2. WSUS Konfigürasyonu

### 3.2.1. WSUS Arayüzünün Açılması

WSUS yönetim ara yüzünü açmak için sunucuda Start butonuna tıklanır. All Programs kısmından Administrative Tools seçilir. Administrative Tools altında bulunan Microsoft Windows Server Update Services kısayolu seçilerek yönetim ara yüzüne ulaşılır.

### 3.2.2. Güncellemelerin Temin Edilmesi

Güncellemeleri Microsoft Update sitesinden indirmeden önce hangi güncellemelerin indirileceği tespit edilmelidir. Bu işlem için iş adımları aşağıdaki gibidir;

- Güncellemelerin indirileceği sunucunun seçimi
- İndirilecek güncellemelere ait dil seçimi
- Hangi ürünler ile ilgili güncelleme indirileceği
- Hangi sınıfa ait güncellemelerin indirileceği
- Güncelleme sıklığının belirlenmesi

### 3.2.3. İnternet Bağlantısı Olmayan Ağlarda Güncelleme:

İnternet bağlantısı olmayan ağlarda güncelleme yapabilmek için Microsoft Update sitesine bağlantı kurabilecek ayrı bir WSUS sunucusuna ihtiyaç vardır. Bu sunucu üzerinde yapılacak yapılandırma ile İnternete bağlı olmayan ağda kullanılan WSUS sunucusunun yapılandırması aynı olmalıdır. İnternete bağlı sunucudan alınan güncellemeler taşınabilir ortamlar (örneğin USB disk) aracılığı ile internet bağlantısı olmayan WSUS sunucusuna taşınmalıdır. İnternete bağlı olan sunucudan indirilen güncellemelerin internete bağlı olmayan WSUS sunucusuna aktarılması için şu işlemler yapılmalıdır. İnternet WSUS sunucusunda gerçekleştirilecek işlemler;

- İnternet sunucusu üzerinde Start menüsünden Run seçilir.
- Gelen kutuya cmd yazılır ve OK seçilir.
- Açılan Command prompt penceresinde `cd \Program Files\Update Services\Tools` yazılarak ilgili dizine geçilir.
- Bu dizinde `wsusutil.exe export paket.cab kayıt.log` komutu çalıştırılır. Burada `paket.cab` ve `kayıt.log` dosyalarının isimleri uygun şekilde değiştirilebilir (örneğin `paket_%tarih%.cab` ve `kayıt_%tarih%.log` gibi).



# TALİMAT

## YAMA GÜVENLİĞİ

BŞEÜ-BİDB Belge No	BGYS.TLM.08
İlk Yayın Tarihi/Sayısı	03.09.2018
Revizyon Tarihi	18.10.2022
Revizyon No	01
Sayfa No	3/3

- Güncellemelerin bulunduğu WsusContent dizini (örneğin D:\WSUS\WsusContent) ve bir önceki adımda oluşturulan paket.cab dosyası harici bir ortama alınır ve internete bağlı olmayan WSUS sunucusuna aktarılır.

İnternete bağlı olmayan WSUS sunucusunda gerçekleştirilecek işlemler;

- Harici ortamdaki Wsus Content dizini WsusContent dizinine (örneğin E:\WSUS\WsusContent) kopyalanır. Kopyalama sırasında var olan dosyalar yenileriyle değiştirilir.
- Harici ortamdaki paket.cab dosyası C:\Program Files\Update Services\Tools altına kopyalanır.
- Start menüsünden Run seçilir.
- Gelen kutuya cmd yazılır ve OK seçilir.
- Açılan Command prompt penceresinde cd \Program Files\Update Services\Tools yazılarak ilgili dizine geçilir.
- Burada wsusutil.exe import paket.cab kayıt.log komutu çalıştırılarak güncelleştirmeler veritabanına yazılır. Son olarak WSUS yönetim arayüzü açılarak yeni eklenen güncelleştirmeler yükleme için onaylanır.

### 3.2.4. İstemcilerin Yapılandırılması

İstemciler aktif dizin kullanılan ortamlarda grup politikaları ile yapılandırılabilir. Aktif dizin kullanılmayan ortamlarda yerel güvenlik politikaları (local security policy) ile veya kütük (registry) değerlerin değiştirilmesi ile istemciler yapılandırılabilir.

### 3.2.5. Güncellemelerin Yönetimi

Güncellemelerin yönetimi, güncellemelerin listelenmesi ve onaylanması/reddedilmesi işlemlerinden oluşmaktadır. Veritabanında kaydı olan güncelleştirmelerin görüntülenmesi için WSUS yönetim ara yüzü açılır. Daha sonra sol tarafta bulunan ağaç yapısında sunucunun altındaki Updates bölümü açılır ve All Updates bölümü seçilir. Gelen sayfanın üst tarafında bulunan Approval ve Status seçeneklerinden görüntülenmek istenen güncelleştirmelere uygun değerler seçilerek Refresh butonuna basılır.

### 3.2.6. Güncelleme Bilgilerinin Raporlanması

Güncelleştirmelerin durumu ile ilgili rapor üretmek için WSUS yönetim ara yüzünün sol tarafındaki menüden Reports bölümü seçilir. Ortada bulunan Update Reports bölümünden istenen rapor tipi seçilir. Burada 3 rapor seçeneği bulunmaktadır.

- Update Status Summary: Bu raporda her bir güncelleştirme için bir sayfalık özet rapor oluşturulur.
- Update Detailed Status: Bu raporda her bir güncelleştirme için tüm bilgisayarların durumunu gösteren bir rapor oluşturulur.
- Update Tabular Report: Bu raporda her bir güncelleştirme için bir satır içeren özet rapor oluşturulur. Bu rapor tipi bilgileri başka formatlara aktarmak için uygundur.

## 4. REFERANSLAR

- Ağ ve Erişim Güvenliği Politikası BGYS.PLT.02