FOX DSS

TEKNİK GÜVENLİK BÜLTENİ

22 EKİM 2026 / REV. 04

PHP2Shell

Kontrol, güncelleme ve geçici yapılandırma rehberi

CVE-2026-109618 / CVE-2026-109619

PHP'de iki kritik güvenlik açığı yayımlandı (**CVSS 9.2**). Kimlik doğrulama gerektirmeden kod çalıştırma WordPress, Drupal ve Joomla üzerinde gösterildi. İnternete açık ve **iç ağdaki** PHP-FPM, Apache/mod_php, CGI, FrankenPHP ve LiteSpeed kurulumları etkileniyor. CMS veya eklenti güncellemesi PHP'nin kendisini güncellemez. [1, 5]

ÖNCELİKLİ AKSİYON

Kalıcı çözüm, kullandığınız PHP sürümünün güvenlik güncellemesini yüklemektir.

PHP 8.2	PHP 8.3	PHP 8.4	PHP 8.5
8.2.35	**8.3.36**	**8.4.27**	**8.5.12**

PHP'nin yayımladığı düzeltilmiş sürümler. Linux paketlerinde numara farklı olabilir, paketin yamayı içerdiğini kontrol edin. [1]

01 Sürümü doğru yerden kontrol edin

WordPress
Araçlar → Site Sağlığı → Bilgi → Sunucu → PHP sürümü
Plesk / cPanel → Alan adının PHP ayarları

Özel uygulama / container
Sitenin kullandığı sürümü her sunucuda kontrol edin.
php -v komut satırını gösterir, site farklı olabilir.

PHP 8.1 ve daha eski sürümlerde, barındırma sağlayıcınıza bu yamanın eklenip eklenmediğini sorun. Eklenmediyse desteklenen bir sürüme geçiş planlanmalı. Güncellemeden sonra PHP servislerini yeniden başlatıp sitedeki sürümü tekrar kontrol edin. Geçici olarak **memory_limit = -1** yaptıysanız eski değerine döndürün. [1, 5]

02 Hemen güncelleyemiyorsanız

Aşağıdaki ayarlar riski azaltır ancak tam koruma sağlamaz. Önce test ortamında uygulamanızla uyumunu deneyin. Değişikliği sistem yöneticinizin yapması önerilir. [1]

BELLEK TÜKENMESİ

CVE-2026-109618

```
memory_limit = -1
```

Ayar php.ini, FPM veya Apache düzeyinde yapılmalı ve başka bir ayar bu sınırı geri getirmemeli. Bellek kullanımı **container veya cgroup sınırıyla** denetlenmeli, bu durumda kesinti yaşanabilir. **RLIMIT_AS ve RLIMIT_DATA kullanılmamalı.** [2]

post_max_size dosya yükleme yoksa **8M**, varsa **32M** olmalı. **upload_max_filesize** bu değerin altında kalmalı. Proxy'de istek boyutu sınırı ve düşük **max_input_nesting_level** önerilir. [1, 5]

İSTEKLER ARASI KALAN VERİ

CVE-2026-109619

```
session.upload_progress.enabled=0
```

Ayar **php.ini** veya FPM havuzunda yapılmalı, **ini_set()** ve **.user.ini** yeterli olmaz. Sonra tüm PHP işlemleri yeniden başlatılmalı. [1,3]

```
fatal_error_backtraces = 0
```

Yalnız PHP 8.5 için. Ayardan sonra servis yeniden başlatılmalı. Hatalı INI ayarları, fatal error ve zaman aşımı hatalarının kaynağı da giderilmeli. [1,3]

DİĞER GEÇİCİ ÖNLEMLER

Üretimde **display_errors = 0** olmalı. PHP-FPM **pm.max_requests** düşürülerek işlemler daha sık yenilenebilir, SELinux veya AppArmor etkiyi sınırlar. İnternete açık uygulamalar **Cloudflare WAF arkasına alınabilir.** PHP2Shell kuralları engelleme modunda olmalı ve sunucuya Cloudflare dışından erişim kapatılmalı. **Bu önlemler güncellemenin yerini tutmaz.** [4, 5]

[1] PHP resmî duyuru [2] OOM önlemleri [3] Durum önlemleri [4] Cloudflare [5] php2shell.com

foxdss.com · info@foxdss.com