T. B. M. M.
İYİ PARTİ
GRUP BAŞKANLIĞI
Tarih: 6.11.2026
Sayı: 7519

52859

M. Satuk Buğra KAVUNCU
İstanbul Milletvekili

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

Aşağıda yer alan sorularımın, Ulaştırma ve Altyapı Bakanı Sayın Abdulkadir URALOĞLU tarafından yazılı olarak cevaplandırılmasını saygılarımla arz ederim. 28/10/2026

M. Satuk Buğra KAVUNCU
İstanbul Milletvekili

Geçtiğimiz haftalarda, internet sitelerinin altyapısında yaygın biçimde kullanılan PHP programlama dilinde iki kritik güvenlik açığının yapay zekâ destekli araştırmalar sonucunda tespit edildiği aktarılmıştır. PHP geliştirici ekibi tarafından 21 Ekim 2026 tarihinde yayımlanan güvenlik güncellemeleriyle giderilmeye çalışılan bu açıkların, belirli koşullar altında kimlik doğrulaması olmadan uzaktan kod çalıştırılmasına imkân verebildiği belirtilmiştir. On yılı aşkın süredir fark edilmeden kaldığı bildirilen bu açıklar, dijital altyapılarda kullanılan yazılımların düzenli olarak denetlenmesinin ve güvenlik güncellemelerinin zamanında uygulanmasının önemini bir kez daha ortaya koymuştur.

Türkiye Siber Güvenlik Başkanlığı tarafından da kamu kurumları, kritik altyapı işletmecileri ve özel sektör kuruluşları sistemlerini gözden geçirmeleri ve gerekli güvenlik güncellemelerini uygulamaları konusunda uyarılmış, risklerin erken tespiti ve etkilerinin sınırlandırılması amacıyla ulusal ölçekte güvenlik taramaları başlatıldığı açıklanmıştır. Aynı açıklamalarda, e-Devlet Kapısı başta olmak üzere kamunun dijital hizmetlerinde güvenliği olumsuz etkileyen bir sorun tespit edilmediği bildirilmiştir. Bununla birlikte, ulusal ölçekte yürütüldüğü belirtilen taramaların kapsamı, kaç sistemin incelendiği, kaç sistemde güvenlik açığı bulunduğu ve tespit edilen risklerin ne ölçüde giderildiği hakkında ayrıntılı bilgiye ihtiyaç bulunmaktadır.

Söz konusu gelişme, yalnızca belirli bir yazılımın güncellenmesiyle sınırlı değerlendirilemeyecek kadar önemlidir. Kamu kurumlarının internet siteleri, elektronik haberleşme altyapıları, veri merkezleri, barındırma hizmetleri ve kurumların hizmet aldığı üçüncü taraf sistemler farklı yazılım bileşenleri üzerinde çalışmaktadır. Kurumların kullandığı yazılımların ve sürümlerin güncel bir envanterinin bulunmaması, güvenlik güncellemelerinin gecikmesi veya artık desteklenmeyen yazılımların kullanılmaya devam edilmesi, benzer açıkların tespit edilmesini ve giderilmesini güçleştirebilir. Ayrıca bir güvenlik açığının kapatılması, daha önce bu açıktan yararlanılarak sisteme erişilip erişilmediğinin araştırılması ihtiyacını ortadan kaldırmamaktadır.

Yapay zekâ teknolojilerinin güvenlik açıklarını tespit etme kapasitesi siber savunma bakımından önemli fırsatlar sunmaktadır. Bununla birlikte aynı teknolojilerin saldırganlar

tarafından da kullanılabilmesi, kurumların yalnızca bilinen açıkları gidermeye değil, sürekli güvenlik izleme, tehdit analizi, olay müdahalesi ve yazılım güncelleme süreçlerini güçlendirmeye de önem vermesini gerektirmektedir. Türkiye'nin dijital hizmetlerinin ve elektronik haberleşme altyapısının güvenliğinin korunması amacıyla yürütülen çalışmaların kapsamı, sonuçları, kurumlar arasındaki sorumluluk paylaşımı ve alınan tedbirlerin etkinliği hakkında kamuoyunun bilgilendirilmesi gerekmektedir.

Bu bağlamda;

1. PHP programlama dilinde tespit edilen kritik güvenlik açıklarının duyurulmasının ardından Bakanlığınız ve bağlı, ilgili ve ilişkili kuruluşları tarafından hangi teknik incelemeler gerçekleştirilmiştir? Bu incelemelerin kapsamı ve sonuçları nelerdir?

2. Bakanlığınızın ve bağlı, ilgili ve ilişkili kuruluşlarının internet siteleri, dijital uygulamaları ve sunucuları arasında PHP altyapısını kullanan kaç sistem bulunmaktadır? Bunlardan kaçının söz konusu güvenlik açıklarından etkilenme riski taşıdığı belirlenmiştir?

3. Tespit edilen güvenlik açıklarına yönelik yayımlanan güncellemeler, Bakanlığınızın ve bağlı kuruluşlarının sorumluluğundaki sistemlere hangi tarihlerde uygulanmıştır? Güncelleme işlemleri tamamlanmamış sistem bulunmakta mıdır?

4. Bakanlığınızın sorumluluk alanındaki sistemlerde söz konusu açıklar nedeniyle yetkisiz erişim, zararlı kod çalıştırılması, veri kaybı, veri sızıntısı veya hizmet kesintisi tespit edilmiş midir? Tespit edilmişse olayların sayısı, kapsamı ve alınan tedbirler nelerdir?

5. Bakanlığınızın ve bağlı kuruluşlarının kullandığı yazılım bileşenlerini, sürümlerini ve güvenlik güncelleme durumlarını gösteren güncel bir envanter bulunmakta mıdır?

6. Bu envanterin düzenli olarak güncellenmesi ve kurumlar arasında koordineli biçimde kullanılması nasıl sağlanmaktadır?

7. Üretici tarafından artık desteklenmeyen veya güvenlik güncellemesi almayan yazılım sürümlerini kullanan sistemler tespit edilmiş midir?

8. Bu sistemlerin güncellenmesi veya yenilenmesi için hangi takvim belirlenmiş, geçiş sürecinde hangi güvenlik önlemleri alınmıştır?

9. Siber güvenlik açıklarının yapay zekâ destekli araçlarla daha erken tespit edilebilmesi amacıyla Bakanlığınız ve Bilgi Teknolojileri ve İletişim Kurumu tarafından yürütülen bir çalışma bulunmakta mıdır?

10. Bakanlığınız, Bilgi Teknolojileri ve İletişim Kurumu ve Siber Güvenlik Başkanlığı arasında kritik yazılım açıklarının bildirilmesi, ulusal ölçekte taranması, giderilmesinin izlenmesi ve sonuçların değerlendirilmesine ilişkin hangi koordinasyon mekanizmaları bulunmaktadır?