YENİ PARTİ
T.B.M.M.
YENİ PARTİ
Grup Başkanlığı
Tarih : 6 Kasım 2026
Sayı : 1671

52727

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

Aşağıdaki sorularımın Cumhurbaşkanı Yardımcısı Sayın Cevdet YILMAZ tarafından Anayasanın 98. Maddesi ve TBMM İçtüzüğünün 96. Maddesi gereğince yazılı olarak cevaplandırılmasını arz ederim. 05.11.2026

Okan KONURALP
Ankara Milletvekili

İnternet siteleri için web tabanlı uygulamalar geliştirmek amacıyla tasarlanmış, açık kaynaklı ve sunucu taraflı çalışan PHP (Hypertext Preprocessor) programlama dilinde "PHP2Shell" olarak adlandırılan CVE-2026-109618 ve CVE-2026-109619 numaralı iki kritik güvenlik açığı meydana gelmiştir. Bu açıkların, saldırganların kimlik doğrulaması olmaksızın sunucularda uzaktan kod çalıştırmasına imkân tanıdığı belirtilmektedir. Ortaya çıkan kritik güvenlik açıkları nedeniyle İngiltere, Hollanda, Fransa, Finlandiya ve Danimarka kamu internet sitelerini önlem olarak geçici süreyle erişime kapatmış; ABD, Japonya, Güney Kore, Çin ve Avrupa Birliği ise acil güncelleme çağrısında bulunmuştur. Cumhurbaşkanlığı Siber Güvenlik Başkanlığı konu hakkında ulusal ölçekte tarama başlattığını belirterek, TR-26-1372 numaralı güvenlik bildirimini yayımlamış tüm kurum ve kuruluşlar ile kritik altyapılara acil bildirim göndermiştir. Aynı zamanda "Dijital altyapılarımızın güvenliği ve kritik hizmetlerin sürekliliği için ulusal düzeyde koordinasyon ve önleyici güvenlik çalışmalarımız sürmektedir." açıklamasını yapmıştır. Basındaki haberlere göre 23 Ekim itibarıyla Türkiye'de 364 bini aşkın hizmet hâlâ etkilenen PHP sürümlerinde çalışmaktadır. Bu krizle alakalı ülkemizde atılan adımların şeffaf biçimde kamuoyuyla paylaşılması gerekmektedir.

Bu bağlamda,

1- Siber Güvenlik Başkanlığı, PHP2Shell olarak adlandırılan güvenlik açığından ilk kez ne zaman ve hangi kanaldan haberdar olmuştur? 21 Ekim 2026 tarihindeki duyurudan önce yabancı muhataplardan ya da PHP geliştirici ekibinden Başkanlığa herhangi bir ön bilgilendirme ulaşmış mıdır?

52727

2- PHP2Shell güvenlik açığı nedeniyle İngiltere, Hollanda, Fransa, Finlandiya ve Danimarka gibi ülkelerde kamu internet siteleri önlem amacıyla erişime kapatılmışken ülkemizde böyle bir tedbir uygulanmaması hangi risk değerlendirmesine dayanmaktadır?

3- Kamu kurum ve kuruluşlarının kullandığı yazılımları ve sürümlerini gösteren merkezi bir envanter tutulmakta mıdır? Tutuluyorsa kamuda PHP tabanlı kaç sistem bulunmaktadır ve bu envanter en son ne zaman güncellenmiştir?

4- Siber Güvenlik Başkanlığı 21 Ekim 2026 tarihinde ulusal ölçekte tarama başlatmış ve TR-26-1372 numaralı güvenlik bildirimiyle kurumları acil güncellemeye çağırmıştır. Bu tarama kapsamında kaç kamu kurumu ve kritik altyapı sisteminde etkilenen PHP sürümü tespit edilmiş, bunların kaçında güncelleme tamamlanmıştır? Güncellemesi tamamlanmayan sistemler için bir süre belirlenmiş midir ve bu süreye uymayan kurumlar hakkında ne tür bir işlem yapılacaktır?

5- Siber Güvenlik Başkanlığına bu veri açığı ile ilgili kaç olay bildirimi yapılmış, bunların kaçında doğrulanmış bir veri ihlali tespit edilmiştir? Kurumlara, sistemlerini güncellemenin yanı sıra geçmiş kayıtlarını da incelemeleri yönünde bir talimat verilmiş midir?