

Saldırı Önleme Sistemlerinde Yüksek Öncelikli Güvenlik Açığı

GamaSEC Bilgi Güvenliği Denetim ve Danışmanlık Servisleri, günümüz ağlarında sıkça kullanılan saldırı tespit / önleme sistemlerinde ve web uygulama güvenlik duvarlarında yüksek öncelikli bir güvenlik açığı buldu. Güvenlik açığının etkin olarak pazarda bulunan çok sayıda ürünü etkilediği saptandı. Güvenlik açığını kullanan bir saldırgan, saldırılarını tamamen gizleyebilmekte ve saldırı önleme sistemlerini atlatabilmektedir.

GamaSEC'in GamaTEAM olarak bilinen denetim ve danışmanlık ekibi, yapmış oldukları güvenlik denetimleri esnasında Nisan 2007 itibariyle çok sayıda saldırı tespit ve önleme sisteminde yüksek öncelikli bir güvenlik açığı saptadı. Güvenlik açığı, evrensel dil kodlamasının farklı bir kullanımı ile saldırı önleme sistemlerinin atlabılabilmesine imkan sağlıyor.

Güvenlik açığının sanılandan daha tehlikeli olduğu ve bilinen saldırıların dahi gizlenebilmesine imkan verdiği bağımsız danışmanlarca doğrulandı. GamaTEAM üyelerinin katkıları ile ilgili ürünleri kullanan müşterilerin, güvenlik açığından en az düzeyde etkilenmesi için, etkilenen ürünlerin üreticileri doğrudan ve diğer üreticiler ise bilgisayar acil durum müdahale ekibi (CERT) aracılığıyla uyarıldı ve çeşitli güvenlik yamaları hazırlandı.

Kurumsal ağlarında saldırı tespit ve önleme sistemi barındıran kurumların, ivedilikle üreticiler ile temasa geçmesi ve sunulan çözüm yöntemlerini uygulaması gerekmektedir.

GamaSEC Bilgi Güvenliği Denetim ve Danışmanlık Servisleri
<http://www.gamasec.net>

GS07-01 Tam/Yarım Genişlikteki Evrensel Dil Kodlaması ile Saldırı Tespit ve Önleme Sistemlerinin Aşılması
<http://www.gamasec.net/gs07-01.html>

CERT - Vulnerability Note VU#739224
<http://www.kb.cert.org/vuls/id/739224>