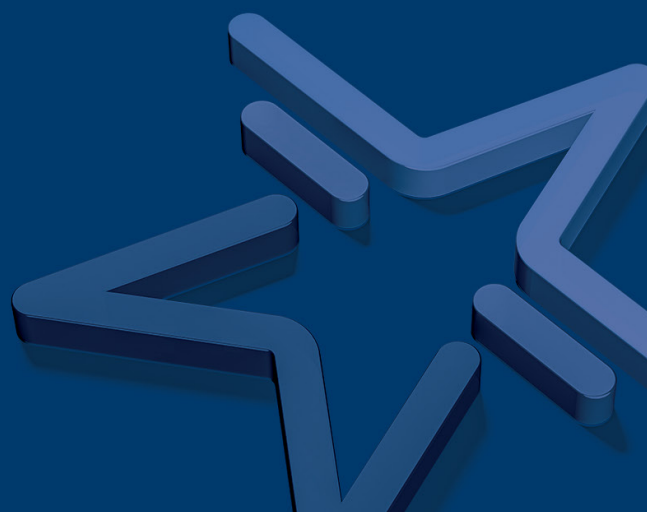
HAVELSAN DIGITAL

Think Future

SİBER GÜVENLİK BÜLTENİ

OCAK 2022

SİBER GÜVENLİK DİREKTÖRLÜĞÜ



www.HAVELSAN.com.tr

HAVELSAN DIGITAL

3 WordPress Eklentisinde Yüksek Önemli Güvenlik Açığı

Feyzi Yuşa KARABABA
Siber Güvenlik Mühendisi
Siber Güvenlik Direktörlüğü

3 WordPress Eklentisinde Yüksek Önemli Güvenlik Açığı

Zafiyet Genel Bilgi

Siber güvenlik araştırmacıları tarafından üç farklı WordPress eklentisinde güvenlik açığı keşif edildi. Bu keşif ile 84.000 kullanıcının risk durumunda olduğu bildirildi.

Wordpress güvenlik şirketi olan wordfence ekibinin geçen haftalarda yayınladığı raporunda "Zafiyet, site yöneticisini kandırıp bir bağlantıya gitmesi ile saldırganın site seçeneklerini değiştirebilmesini mümkün kılmaktadır." yazdı.

CVE-2022-0215 kaydını alan zaafiyet, siteler arası istek sahteciliği (CSRF) zafiyeti CVSS ölçeğinden 8.8 (Yüksek) risk değerlendirmesi aldı. Xootix tarafından sağlanan 3 eklentiler;

- Login/Register Popup
- Side Cart Woocommerce
- Waitlist Woocommerce

OWASP belgelerinde "Kurban yönetici hesabı ise, CSRF zafiyet tüm web uygulamasını tehlikeye atabilir" demektedir.

Spesifik olarak, güvenlik açığının kaynağı Ajax isteklerini işlerken doğrulama eksikliğinden kaynaklanmaktadır, saldırganın bir web sitesinde "user_can_register" (Herkes kaydolabilir) seçeneği doğru olarak güncelleyebilmesine ve "default_role" (bloğa kaydolan kullanıcıların varsayılan rolü) ayarını yapmasına olanak sağlar.

Login/Register Popup eklentisi 20.000'den fazla sitede kurulu iken, Side Cart Woocommerce ve Waitlist Woocommerce sırası ile 4.000 ve 60.000'den fazla web sitesine yüklenmiştir. Wordfence araştırmacıları tarafından 5 Kasım 2021 tarihinde yapılan açıklamanın ardından, bu zaafiyet Login/Register Popup eklentisinde 2.3, Side Cart Woocommerce eklentisinde 2.1 ve Waitlist Woocommerce eklentisinde 2.5.2 sürümlerinde ele alınmıştır.

```php
public function save_settings(){

    if( !current_user_can( $this->capability ) ) return;

    $formData = array();

    $parseFormData = parse_str( $_POST['form'], $formData );

    foreach ( $formData as $option_key => $option_data ) {

        $option_data = array_map( 'sanitize_text_field', stripslashes_deep( $option_data ) );

        update_option( $option_key, $option_data );

    }

    wp_send_json(array(
        'error'     => 0,
        'notice'    => 'Settings Saved',
    ));
}
```

Etki Alanı

WordPress Login/Register Popup, Side Cart Woocommerce ve Waitlist Woocommerce eklentisinden her hangi birini kullanan WordPress kullanıcıları

Önerilen Güvenlik Önlemleri

- Login/Register Popup eklentisini 2.3 sürümüne yükseltmek
- Side Cart Woocommerce eklentisini 2.5.2 sürümüne yükseltmek
- Waitlist Woocommerce eklentisini 2.1 sürümüne yükseltmek

Referanslar

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0215

https://thehackernews.com/2022/01/high-severity-vulnerability-in-3.html

https://www.wordfence.com/blog/2022/01/84000-wordpress-sites-affected-by-three-plugins-with-the-same-vulnerability/

HAVELSAN
DIGITAL

SolarWinds Serv-U Login Paneli Zafiyeti

Regaip KURT
Siber Güvenlik Uzmanı
Siber Güvenlik Direktörlüğü

www.HAVELSAN.com.tr

SolarWinds Serv-U Login Paneli Zafiyeti

Zafiyet Genel Bilgi

Log4J zafiyetinin duyurulmasının ardından saldırganların bu kütüphaneyi kullanan uygulamalara sömürmeye çalıştığı görülmektedir. Açıklığı gidermek için gelen güncellemelerde de ard arda zafiyetler tespit edilmiş, son olarak kütüphanenin 1.17.1 sürümü yayınlanmıştır. Bu süre zarfında kütüphaneyi kullanan birçok uygulama da güncellenmeye devam etmektedir.

Son olarak Microsoft araştırmacıları tarafından SolarWinds dosya paylaşım yazılımı Serv-U üzerinde yetersiz girdi doğrulamadan kaynaklanan ve Log4J akışlarını kullanan bir açıklık olduğu belirtilmiştir. Log4J sömürü saldırılarını takip eden Microsoft ekibi serv-u.exe dosyasından kaynaklanan saldırılar görmüş ve incelemeler sonucunda web giriş ekranı üzerinden alınan temizlenmeyen kullanıcı girdisinin LDAP sorguları çalıştırmak için kullanıldığını tespit etmiştir.

Saldırının başarılı olup olmadığı konusunda bilgi paylaşmayan Microsoft ekibi, kullanıcılarını gerekli yamaları yapmaları konusunda uyarmıştır. SolarWinds uygulamanın Log4J kütüphanesini kullanmadığını belirtmiş ve Serv-U üzerindeki yetersiz girdi doğrulama problemini çözmek için güncelleme yayınlamıştır.

Açıklığın Log4J zafiyeti olup olmadığı belli olmasa da yetersiz girdi doğrulama problemi CVE-2021-35247 koduyla duyurulmuştur.

Önerilen Güvenlik Önlemleri

SolarWinds Serv-U yazılım güncellemelerini gerçekleştirmek. Sorun 15.3 versiyon güncellemesi ile çözülmüştür.

Referanslar

https://nvd.nist.gov/vuln/detail/CVE-2021-35247

HAVELSAN
DIGITAL

VMWare Kimlik Doğrulama Yazılımında SSRF Güvenlik Açığı

Muhammet KARAALİ
Siber Güvenlik Mühendisi
Siber Güvenlik Direktörlüğü

www.HAVELSAN.com.tr

VMWare Kimlik Doğrulama Yazılımında SSRF Güvenlik Açığı

Zafiyet Genel Bilgi

Araştırmacılar, VMWare kimlik doğrulama yazılımı sürümlerinde sunucu taraflı bir istek sahteciliği (SSRF) güvenlik açığının bir saldırganın yönetimsel JSON Web Belirteçlerini (JWT) almasına izin verebileceği konusunda uyarmaktadır.

Çok faktörlü kimlik doğrulama, koşullu erişim ve SaaS, web, mobil uygulamalarda tek seferlik oturum açmayı sağlayan SSRF zafiyeti VMware Workspace ONE Access'de (eskiden Identity Manager olarak biliniyordu) bulunmaktadır.

CVSS puanı 7.5 olan ve yüksek önem derecesine sahip (CVE-2021-22056) güvenlik açığı, ağ erişimine sahip kötü niyetli bir aktörün rastgele kaynaklara HTTP istekleri yapmasına ve tam yanıtı okumasına olanak sağlayabilmektedir.

Assetnote firmasının 17 Ocak blog gönderisinde şöyle yazmaktadır: "Eğik çizgi karakterinin olmaması nedeniyle, bir saldırganın rastgele kaynaklara HTTP istekleri yapması ve tam yanıtı okuması mümkün olmaktadır.

Ayrıca, bir yetkilendirme başlığı sızdırılabilmekte ve bu nedenle bir saldırgan bir resmi görüntüleyerek veya tek bir tıklama yaparak bir yöneticinin yetkilendirme başlığını çalması mümkün olmaktadır."

Zafiyeti keşfeden araştırmacılar Shubham Shah ve Keiran Sampson, bunun JWT'lerin sızdırılmasına yol açabileceğini ve potansiyel olarak kötü niyetli bir aktörün savunmasız bir sisteme tam erişime izin verebileceğini söylemektedir.

Önerilen Güvenlik Önlemleri

VMware Workspace ONE Acces 21.08.0.1 ve Identity Manager'ın 4.6.540.0 sürümlerine güncellenmesi gerekmektedir.

Etkilenen Sistemler

VMware Workspace ONE Access 21.08, 20.10.0.1,20.10 ve Identity Manager 3.3.5, 3.3.4,3.3.3 sürümleri

Referanslar

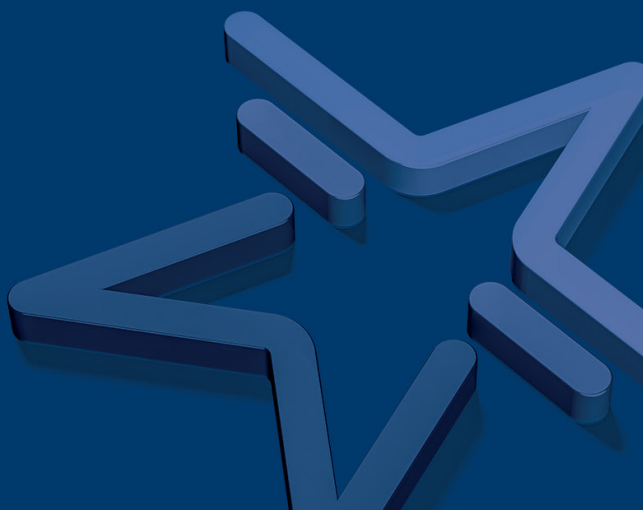
https://portswigger.net/daily-swig/ssrf-vulnerability-in-vmware-authentication-software-could-allow-access-to-user-data

https://nvd.nist.gov/vuln/detail/CVE-2021-22057

https://nvd.nist.gov/vuln/detail/CVE-2021-22056

HAVELSAN
DIGITAL

Think Future



www.HAVELSAN.com.tr