SİBER GÜVENLİK GÜNDEMİ

7.Hafta Siber Güvenlik Haberleri

Beyaz Net
Bilişim partneriniz

İçindekiler

Haftanın Exploitleri

Tarih	Exploit Başlığı	Tür	Platform
12-02-2021	PDFCOMPLETE Corporate Edition 4.1.45 - 'pdfcDispatcher' Unquoted Service Path	Local	Windows
15-02-2021	Teachers Record Management System 1.0 - 'searchteacher' SQL Injection	WebApps	PHP
16-02-2021	BlackCat CMS 1.3.6 - 'Display name' Cross Site Scripting (XSS)	WebApps	PHP
17-02-2021	Batflat CMS 1.3.6 - Remote Code Execution (Authenticated)	WebApps	PHP
18-02-2021	Billing Management System 2.0 - 'email' SQL injection Auth Bypass	WebApps	PHP

Güncel tüm exploitlere buradan ulaşabilirsiniz.

Haftanın Zafiyetleri

Tarih	Zafiyet Başlığı	Zafiyet Türü
16-02-2021	CVE-2021-1801	Zero-Day
17-02-2021	CVE-2020-25605	Eksik Şifreleme

Şubat ayı içerisinde yayınlanan tüm zafiyetlere buradan ulaşabilirsiniz.

Haftanın Zararlı Yazılımları

Tarih	Zararlı Yazılım Başlığı	Tür/Platform
17-02-2021	APOMacroSploit	E-posta Kampanyası

Haber Yazısı 1

Yandex Mail Veri İhlali

TARİH: 12 Şubat 2021

Rusya'nın Hollanda'da menşeili arama motoru, araç çağırma ve e-posta hizmeti sağlayıcısı Yandex, cuma günü kullanıcılarının 4.887 e-posta hesabını tehlikeye atan bir veri ihlalini açıkladı.

Şirket, kişisel kazanç için kullanıcıların posta kutularına yetkisiz erişim sağlayan isimsiz bir çalışanı olay için suçladı.

Şirket, güvenlik ihlalinin sistemlerinde güvenlik ekibi tarafından yapılan rutin bir denetim sırasında tespit edildiğini söyledi. Ayrıca, olay sırasında kullanıcı ödeme ayrıntılarının tehlikeye atıldığına dair hiçbir kanıt olmadığını ve etkilenen posta kutusu sahiplerine şifrelerini değiştirmeleri için bildirimde bulunduğunu söyledi. İhlalin ne zaman meydana geldiği veya çalışanın üçüncü şahıslara yetkisiz erişim sunmaya başladığında şimdilik belli değil.

Şirket, "Olayla ilgili kapsamlı bir iç soruşturma yürütülüyor ve Yandex, idari erişim prosedürlerinde değişiklikler yapacak . Bu, bireylerin gelecekte kullanıcı verilerinin güvenliğini tehlikeye atma potansiyelini en aza indirmeye yardımcı olacaktır. Şirket ayrıca kolluk kuvvetleriyle de iletişime geçti." dedi .

Bu, içeriden gelen tehditlerin teknoloji şirketlerini rahatsız ettiği ve finansal veya itibar zararına yol açtığı ilk olay değil maalesef.

[1] Haber ayrıntılarına buradan ulaşabilirsiniz.

Haber Yazısı 2

Telegram İle Gönderilen Bir Çıkartma Gizli Sohbetlerinizi Açığa Çıkarmış Olabilir

TARİH: 15 Şubat 2021

Siber güvenlik araştırmacıları pazartesi günü, Telegram mesajlaşma uygulamasında, kullanıcıların gizli mesajlarını, fotoğraflarını ve videolarını uzaktaki kötü niyetli kişilere ifşa edebilecek, şimdi yamalanmış bir kusurun ayrıntılarını açıkladı.

Sorunlar İtalya merkezli Shielder tarafından uygulamanın iOS, Android ve macOS sürümlerinde keşfedildi . Sorumlu açıklamanın ardından Telegram, 30 Eylül ve 2 Ekim 2020 tarihlerinde bir dizi yama ile bunlara hitap etti.

Kusurlar, gizli sohbet işlevinin çalışma şeklinden ve uygulamanın animasyonlu çıkartmaları işlemesinden kaynaklanıyordu , böylece saldırganların şüphesiz kullanıcılara hatalı biçimlendirilmiş etiketler göndermelerine ve hem klasik hem de Telegram kişileriyle paylaştıkları mesajlara, fotoğraflara ve videolara erişmelerine olanak tanıyor.

Dikkat edilmesi gereken bir nokta, günümüzde modern cihazlarda güvenlik savunmalarını aşmak için yukarıda belirtilen zayıflıkları en az bir ek güvenlik açığına zincirlemeyi gerektirdiğinden, doğada kusurlardan yararlanmanın önemsiz olmayabileceğidir. Bu kulağa yasak gelebilir, ancak tam tersine, hem siber suç çetelerinin hem de ulus-devlet gruplarının ulaşabileceği yerlerdedir.

Shielder, kullanıcılara cihazlarını güncellemeleri için yeterli zaman vermek amacıyla hataları kamuya açıklamadan önce en az 90 gün beklemeyi seçtiğini söyledi.

Araştırmacılar , "Periyodik güvenlik incelemeleri, özellikle animasyonlu etiketler gibi yeni özelliklerin piyasaya sürülmesiyle yazılım geliştirmede çok önemlidir. Bildirdiğimiz kusurlar, bir saldırıda siyasi muhaliflerin, gazetecilerin veya muhaliflerin cihazlarına erişmek için kullanılmış olabilir." dedi .

Telegram'ın gizli sohbet özelliğinde ortaya çıkan ikinci kusurun , macOS uygulamasında geçen haftaki , gizli sohbetlerden kaybolduktan uzun süre sonra kendi kendini yok eden ses ve görüntülü mesajlara erişmeyi mümkün kılan gizliliği bozan bir hataya ilişkin raporların ardından, bunun ikinci kusur olduğunu belirtmek gerekir.
.

Bu ilk kez değil ve mesajlaşma servisleri yoluyla gönderilen multimedya dosyaları hain saldırılar gerçekleştirmek için silah haline getirildi.

[2] Haber ayrıntılarına buradan ulaşabilirsiniz

Haber Yazısı 3

ShareIT Android Uygulama Kusuru

TARİH: 16 Şubat 2021

Bir milyardan fazla indirmeye sahip popüler bir uygulama olan SHAREit'te , bir kullanıcının hassas verilerini sızdırmak, rastgele kod çalıştırmak ve muhtemelen uzaktan kod yürütülmesine yol açmak için kötüye kullanılabilecek birden fazla yamalanmamış güvenlik açığı keşfedildi .

Bulgular, siber güvenlik firması Trend Micro'nun, kullanıcıların cihazlar arasında dosya paylaşmasına veya aktarmasına olanak tanıyan uygulamanın Android sürümünü analizinden geliyor.

Kusurlardan biri, uygulamanın dosya paylaşımını kolaylaştırma biçiminden (Android'in FileProvider aracılığıyla), potansiyel olarak herhangi bir üçüncü tarafın geçici okuma / yazma erişim izinleri almasına ve bunları uygulamanın veri klasöründeki mevcut dosyaların üzerine yazmasına izin vermesinden kaynaklanmaktadır.

29 Haziran 2020'de Hindistan hükümeti, bu uygulamaların "Hindistan'ın ulusal güvenliğini ve savunmasını tehdit eden ve sonuçta Hindistan'ın egemenliğine ve bütünlüğüne zarar veren" faaliyetlerde bulunduğuna dair endişeler nedeniyle diğer 58 Çin uygulamasıyla birlikte SHAREit'i yasakladı.

Şimdilik zafiyetle ilgili herhangi bir açıklama veya danışmanlık belgesi bulunmamakta.

[3] Haber ayrıntılarına buradan ulaşabilirsiniz

Haber Yazısı Kaynakça

1. YandexMail
2. Telegram
3. ShareIT
4. Zararlı Yazılımlar
5. Zafiyetler
6. Exploitler