SCADAfence | Value-Added Distributor OTD BİLİŞİM www.onlineteknikdestek.com

ICT OTD PREFER EXPERIENCE ONLINE Since 2011

Kapsamlı Endüstriyel Cihaz Yamalama Kılavuzu

Maliyetler vs. Faydalar Araştırma Laboratuvarından Bilgiler

SCADAfence Research Biriminin Orijinal Yayını

Ofer Shaked, SCADAfence Kurucu Ortağı ve BTS

Ofer Shaked - Konuşmacı Profili

SCADAfence Kurucu Ortağı ve BTS

- **13 yıllık SCADA / Endüstriyel Güvenlik geçmişi**
- **Eski İsrail Intelligence Elite Siber Birimi Görevlisi**
- **OTCSA'da Mimar**
- **ManuSec Danışma Kurulu üyesi**
- **ICS Güvenlik Konferanslarında Konuşmacı**

İçindekiler Tablosu

Yamalama Maliyeti
1. Adım: Güvenlik Açığı Keşfi

SCADAfence | Value-Added Distributor OTD BILIŞIM www.onlineteknikdestek.com

ICT OTD PREFER EXPERIENCE ONLINE Since 2011

Endüstriyel Cihazların Güvenlik Açığını Yönetme Süreçleri

Güvenlik açığınızın olup olmadığını bilmek için öncellikle varlıklarınızın tümünü incelemeniz gerekir. Daha sonra güvenlik açıklarına ilişkin bu varlıkları değerlendirmelisiniz.

01 Varlık Keşfi

02 Güvenlik Açığı Değerlendirmesi

03 Analiz

04 Çözüm

Vaka Çalışmaları: Güvenlik Açığı Taraması

Vaka Çalışması #1

Almanya'daki Otomotiv Üreticisi

Önemli sunucular tek bir kritik güvenlik açığı taraması ile üretim aşamasında çöktü. Sunucular üretim sürecinin önemli bir parçasıydı ve Hata Vermeleri aksaklığa neden oldu.

Neden: Sunucular paralel olarak yalnızca 4 sokete kadar desteklerken tarayıcı 13 soket açtı.

Vaka Çalışması #2

ABD'deki BMS Operatörü

En iyi 3 Güvenlik Açığı Tarayıcısından biri kullanılarak yapılan ağ genelinde bir tarama sonucunda bina otomasyon sistemlerinin %50'sinden fazlası çöktü.

Düzeltilmesi için etkilenen alanlara birçok sağlayıcının teknisyenlerinin çağrılması gerekti.

Onarımın parasal maliyeti 1 Milyon $ oldu.

Neden: Tarayıcı yaygın kullanımda olmayan ve sağlayıcılar tarafından hedef cihazlarda uygun şekilde test edilmeyen bir Fonksiyonu tetikledi.

Sonuç

Güvenlik taraması OT'de yapılacak tarama işlemi için uygun değildir.

Güvenli Güvenlik Açığı Keşfi için Dört Adım

1. Adım:
Bir Varlık Envanteri Oluşturun (pasif & aktif kaynaklar)

2. Adım:
Hangi varlıkların ulaşılabilir olduğunu ve nereden ulaşılabileceğini anlamak için bir Ağ Haritalandırması yapın.

Kaynak: OTCSA Makalesi: "Operasyonel Teknoloji için Güvenlik Açığı Yönetimi"

3. Adım:
Güvenlik açıkları paylaşım kaynaklarından güvenlik açıkları toplayın.

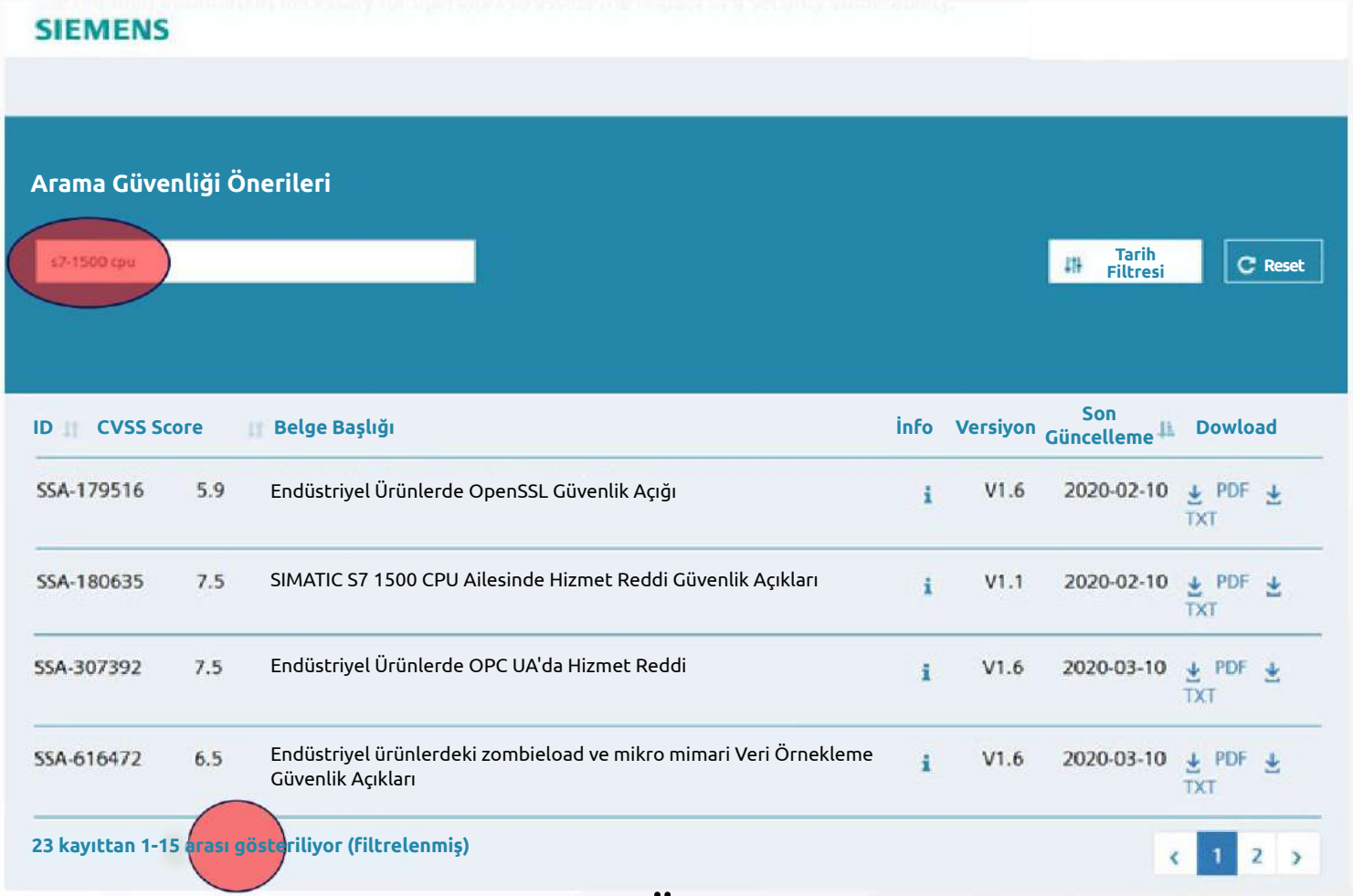
4. Adım:
Varlıklara ilişkin güvenlik açıklarını haritalandırın.

Yamalama Maliyeti

2. Adım: Yama Cihazları

Cihaz Başına kaç yama gereklidir?

Vaka çalışması: Siemens SIMATIC S7-1500 CPU



Kaynak: Siemens Güvenlik Önerileri

23 güvenlik tavsiyesi

Siemens SIMATIC S7-1500 CPU-23 güvenlik önerileri

83 ve yama gerektiriyor

23 girişten 19'u yama gerektiren CPU güvenlik açıklarıdır

Çeşitli güvenlik açıkları

19 girişin bazıları birden fazla güvenlik açığı içermektedir

Bildirim

Ürün, endüstri çapında bir soruna örnek olarak kullanılmakla beraber herhangi bir ürüne veya satıcıya özgü değildir.

Siemens SIMATIC S7-1500 CPU - Gerekli Güvenlik Yamaları

Piyasaya sürüldüğü günden beri 7 yıl içerisinde, yamalamanın güncel tutulması için S7-1500 cihaz başına 13 güncellemeye ihtiyaç duyuldu.

Sonuç: Yamalamanın güncel tutulması her cihazla sık sık ilgilenilmesini gerektirir.

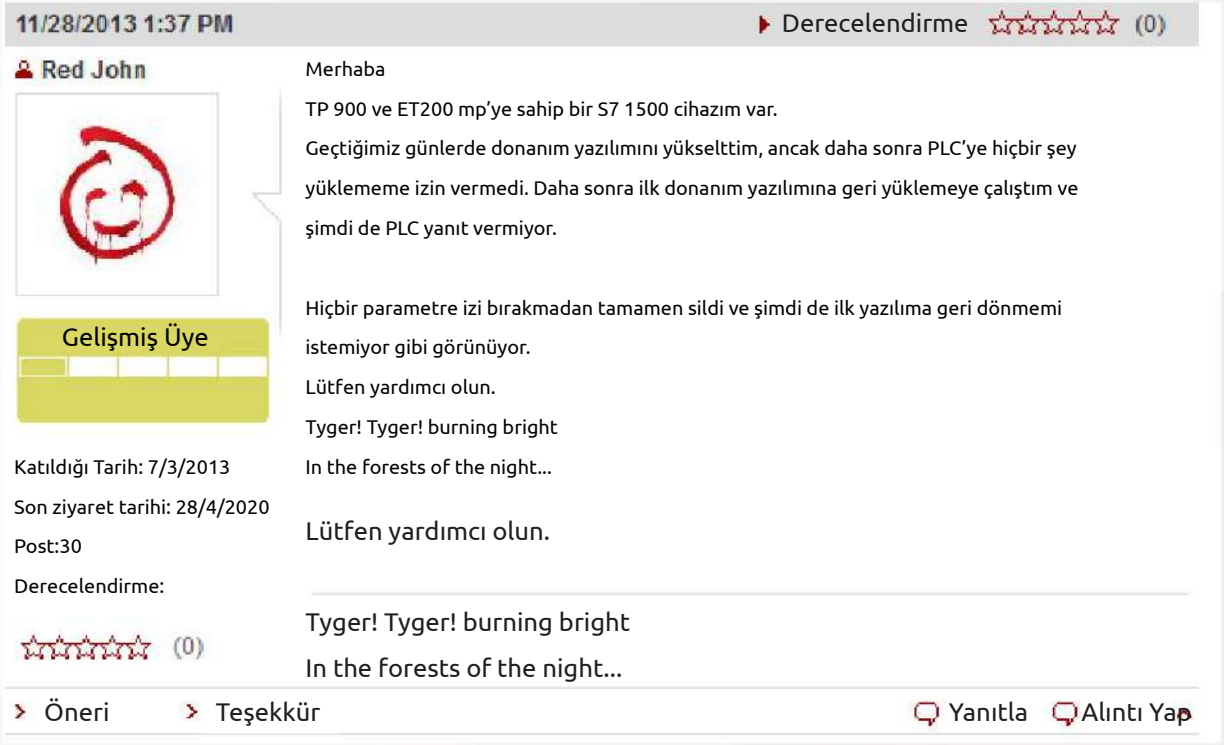
Yama Uygulama Maliyeti -#1

Yükseltme Hatası

Bir kullanıcı Siemens SIMATIC S7-1500 CPU üzerindeki bir donanım yazılımını yükseltmeye çalışmış, neticesinde programı PLC'ye yüklemede bir hata almıştır.

Geri Yükleme Hatası

Kullanıcı geri yüklemeye çalıştığında cihazı bozmuş.



Yama Uygulama Maliyeti -#2

İletişim Kaybı

Başka bir kullanıcı Rockwell Otomasyon / Allen Bradley Micro830 PLC cihazını yamalamaya çalışmış ve cihazla iletişimi kaybetmiştir.

Zaman & Para Kaybı

Bu kendisine 200 $'a mal olmuş ve zamanını boşa harcamasına sebep olmuştur. Büyük bir yama ve bulutun kuruma maliyeti milyonlara ulaşabilir!

Vladimir Romanov • 2nd
McGill MBA 2021 | Control Systems & Automation Consultant | Electrical Engi...
1h •

Bugün Rockwell Otomasyonundan Micro830 ile oldukça ilginç bir deneyim yaşadım.

Meslektaşlarımın birçok pozitif görüşünü okuduktan sonra ben de kendime bir birim almak istedim. Birimi almadan önce (ücretsiz) yazılımı kurdum ve uygun ControlFlash donanım yazılımı değişikliklerini indirdim.

PLC'nin RSinx ağacında hala göründüğüne eminim, ancak artık kullanamıyorum veya iletişim kuramıyorum.

İnternette araştırdıktan sonra, USB üzerinden kullanıldığında bu tür durumların "yaygın olarak ortaya çıktığını" gördüm. Bunun neden olduğu hakkında herhangi bir gösterge veya üretici tarafında herhangi bir çözüm görünmüyor.

Şu anda 200$ bir kağıt tutucuya sahip olmaktan dolayı hayal kırıklığına uğradım.

Bunlar sahada da en az bu kadar güvenilmez midir?

#controls #PLC #automation #Rockwell

Sonuç

Yama Uygulama Maliyeti

Yama uygulama cihazları bozma veya senkronizasyon problemlerine yol açma riski taşır.

Bu da aksaklığa - yani tam olarak kullanıcıların yama ile engellemek istediği şeye sebep olur!

Yamalamanın Faydaları

Araştırma Laboratuvarından Bilgiler Bölüm 1

1

SCADAfence'in ofansif araştırma kolu CVE-2020-13238 ve CVE-2020-12117 gibi endüstriyel ürünlerde güvenlik açıkları tespit etmiştir.

2

Endüstriyel bir bileşende bir güvenlik açığı tespit ettik.

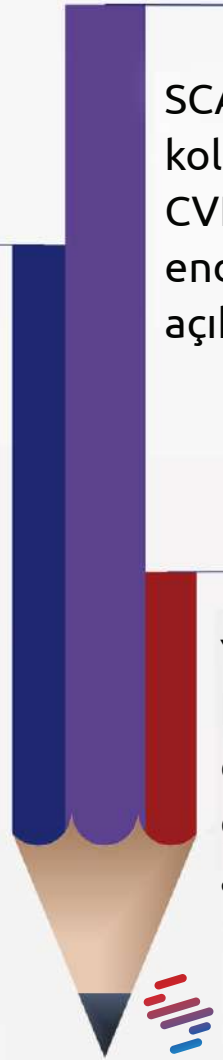
Sağlayıcı bir yama yayınladıktan sonra, biz de bu yamayı test ettik ve yamalanan bileşende benzer bir açıklık tespit ettik.

Bu da genel yama verimliliğini azaltmaktadır."
- Ofer Shaked, SCADAfence Kurucu Ortağı ve BTS

Sonuç

3

Yamaların tümü hem çok genel, hem de çok spesifiktir ve keşfedilecek ve ele alınacak benzer güvenlik açıkları için birçok oda açık bırakır.

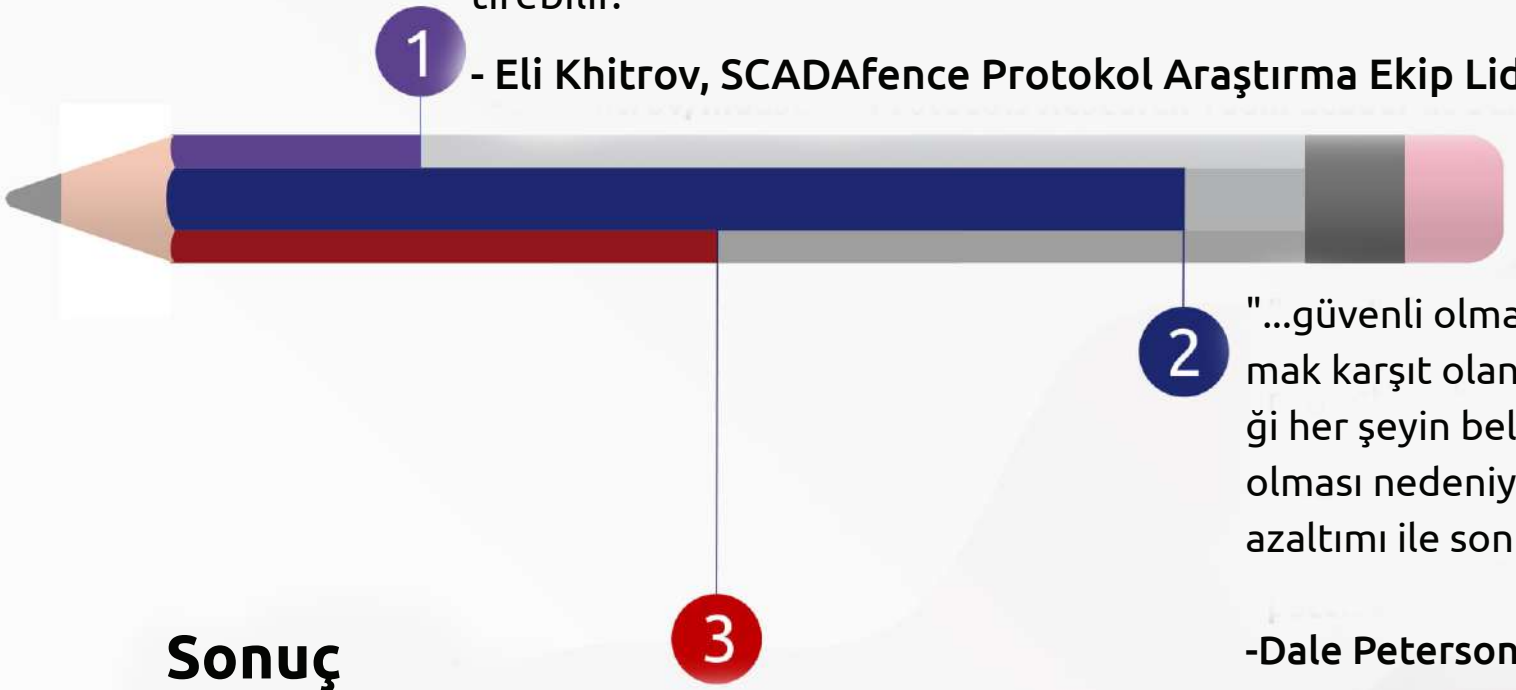


Araştırma Laboratuvarından Bilgiler Bölüm 2

“Birçok endüstriyel cihazın cihaza özel protokollerinde üzerindeki yamaları etkisiz hale getiren temel güvenlik araçları yetersizdir.

Doğrulama nadiren yapılır, dolayısıyla bir saldırgan belgelendirilmeyen her türlü güvenlik açığını kullanmadan istediği işlemi doğrudan gerçekleştirebilir.”

- Eli Khitrov, SCADAfence Protokol Araştırma Ekip Lideri



"...güvenli olmayan bir siber varlığı yamalamak karşıt olanın ihtiyaç duyduğu ve istediği her şeyin belgelendirilmiş bir özellik olması nedeniyle genellikle önemsiz bir risk azaltımı ile sonuçlanır.

-Dale Peterson “Amaçsız Bir İş: ICS’nizdeki her şeyi yamalamaya çalışmak”

Sonuç

Hedef cihazlarda doğrulama gibi temel güvenlik ölçümlerinin yetersiz olması halinde yamalar tamamen etkisiz olabilir.

Sonuçlar

Sonuçlar

Bir Varlık Envanteri Oluşturun

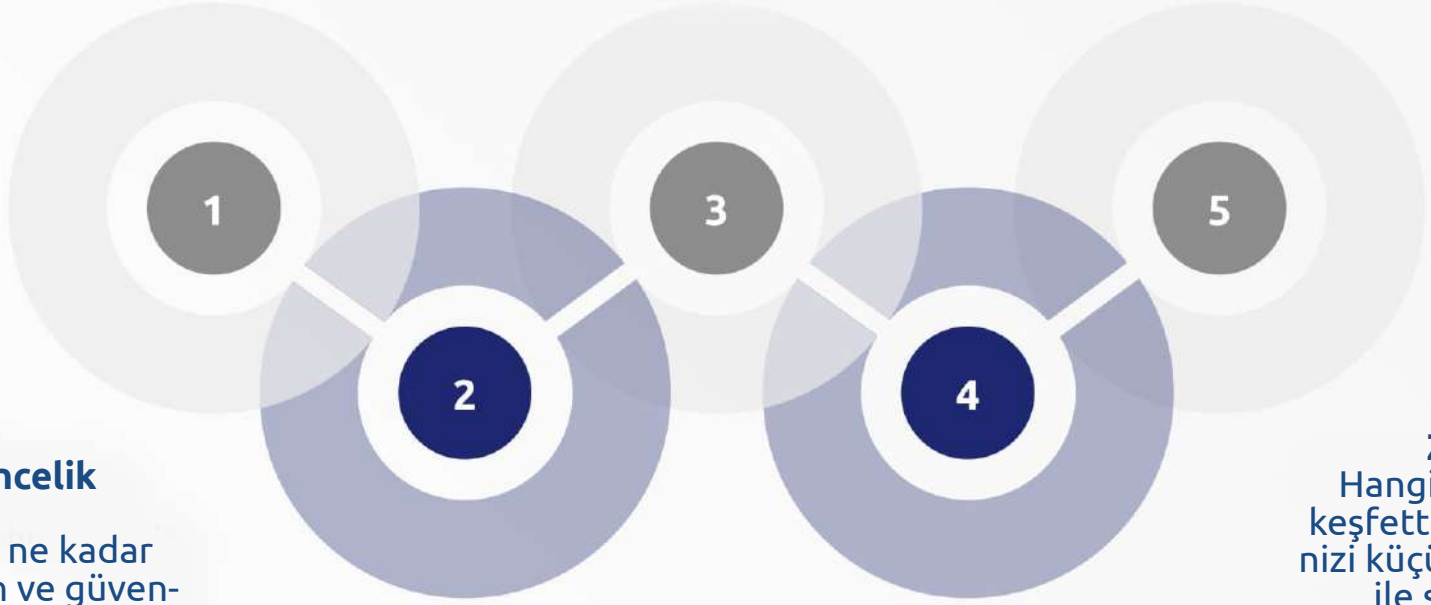
Otomatik, güncel, pasif & aktif varlık envanterleri en büyük kapsamı sunar.

Varlıklara ilişkin Güvenlik Açıklarını Haritalandırın

Güvenlik açığı paylaşım kaynaklarınızı varlık envanterinizle eşleştirerek varlıklara ilişkin güvenlik açıklarını haritalandırın. Endüstriyel cihazların istikrarsızlığı nedeniyle aksaklığı önlemek için güvenlik açıklarını taramaktan kaçının.

İstismarı Tespit Edin

Bazı cihazların geçici veya kalıcı olarak yamalanmamış olarak kalacağını unutmayın. Ağınızdaki güvenlik açıklarının istismarını tespit etmek için araçlar kullanın.



Güvenlik Açıklarını Öncelik Sırasına Koyun

Cihazın ağ tehditlerine ne kadar maruz kaldığını, cihazın ve güvenlik açığının ne kadar önemli olduğunu ve yamanın etkisini anlayın.

Zayıf Cihazları İzole Edin

Hangi cihazların zayıf olduğunu keşfettikten sonra, saldırı yüzeyinizi küçültmek için arayüzlerini ağ ile sınırlandırarak bu cihazları Güvenlik Duvarlarının arkasına almayı düşünün.

Endüstriyel Güvenlik Açığı Yönetim Ekipleri için Bir Karar Alma Aracı

SCADAfence

Value-Added Distributor
OTD BİLİŞİM
www.onlineteknikdestek.com

ICT OTD PREFER EXPERIENCE ONLINE Since 2011

Endüstriyel Güvenlik Açıkları için Karar Alma Aracı

Karar Verme Aracı - Güvenlik Açığı Bilgi Toplama

	Soru	Cevap (1-3 arası)	Yanıt Anlamı
Anında Etki	Bu güvenlik açığından yararlanılması durumunda acil güvenlik / çevre / iş etkisi ne olur?	1-3	1- Düşük 2- Orta 3- Yüksek / Kritik
Diğer Etki	Güvenlik açığından yararlanılması durumunda diğer varlıklar üzerindeki etkisi ne olur?	1-3	1-Diğer varlıklara etkisi yok 2-Kısmi ağ güvenliği ihlali 3-Önemli ağ güvenliği ihlali
Maruz K alma	Etkilenen varlıklar farklı saldırı vektörlerine (ağ tabanlı saldırılar, fiziksel erişim) ne kadar maruz kalıyor?	1-3	1-Yüksek güvenlik bölgesi 2-Ayrıcalıklı / dahili bölge 3-İnternete dönük / halka açık / misafir bölgesi
Olasılık	Bunu sömürülmesi ne derecede kolay?	1-3	1-Sömürülme olasılığı düşük 2-Sömürülme olasılığı yüksek 3-Halihazırda çoğunlukla sömürülmüş durumda
Toplam	12/12		

Daha yüksek puan, güvenlik açığını yamama riskinin daha yüksek olduğunu gösterir.

Karar alma aracı - yama bilgisi toplama

	Soru	Cevap (1-3 arası)	Yanıt Anlamı
Zamanlama	Yama uygulaması kapsamına derhal dahil olan kesinti süresinin maliyeti nedir (yamanın başarılı olduğunu varsayarsak)?	1-3	1-Arıza süresi çok az veya hiç yok 2-Önemli kesinti süresi (yönetilebilir) 3-Daha yüksek yönetim onayı gerektirmektedir
Hatalar	Kimi cihazların (%10'dan fazla olmamak şartı ile) yama uygulamasından kaynaklı olarak işlevlerini kaybetmesi durumunda işletme üzerindeki etkisi ne olur?	1-3	1-Çok az veya hiç etkisi yok 2-Önemli etki 3-Tolere etmesi zor
Stabilite	Aşağıdaki faktörlere bağlı olarak yamanın stabil niteliğinden ne kadar eminsiniz: 1. Yamayı tedarik eden satıcının güvenilirliği nedir? 2. Yama ile bir çekirdek mi yoksa çevresel bir bileşen mi değiştiriliyor? 3. Kaç sürüm üzerinden geçiyorsunuz (daha fazla sürüm - daha fazla hata ihtimali)?	1-3	1-Oldukça emin 2-Emin değilim 3-Yüksek hata olasılığı
Kapsam	Kaç cihaza yama yapmayı planlıyorsunuz? Cihaz sayısı arttıkça kimilerinde arıza olasılığı da o kadar artar.	1-3	1-Bir veya sadece birkaç 2-10-50 3-50'den fazla
Kurtarma	Bazı cihazların işlevselliğini kaybetmesi durumunda bu işlevselliği geri getirme beceriniz (örneğin yedeklemelerden) nedir?	1-3	1-Kolay (ör. Yedeklerim ve yedek cihazlarım var) 2-Önemli çaba; 3-Son derece zor (Örn: yerinde bir satıcıyı aramak zorunda kalmak ya da cihazların kesilmesi / ikame edilmesinin zor olması)
Toplam	15/15		

Daha yüksek puan, güvenlik açığını yamama riskinin daha yüksek olduğunu gösterir.

Örnek Politikalar - Karar Verme Aracını Kullanma

Güvenlik Açığı bilgileri	Yama Bilgileri	Politika
Karşılaşma == 3 ve olasılık> = 2	Her	Şimdi Yama!
Total >=10	Toplam> = 7	Şimdi Yama!
Toplam==4	Toplam> = 7	Dokümanda yama yok

Risk toleransınıza göre kendi politikalarınızı ekleyin

Olgunluk Modeli - Güvenlik Açığı Yönetim Programları

Ek okuma

Bu makalelere bir göz atın

Carnegie Mellon Üniversitesi
Yazılım Mühendisliği Enstitüsü

GÜVENLİK AÇIĞINA YANITLARI ÖNCELİKLENDİRME PAYDAŞLARA ÖZEL BİR KIRILMAZLIK KATEGORİZASYONU

Jonathan M. Spring, Eric Hatleback, Alen Householder, Art Manion, & Deana Shick November 2019

https://resources.sei.cmu.edu/asset_files/WhitePaper/2019_019_001_636391.pdf

ICS Güvenlik Yaması: Asla, Daha Sonra, Şimdi

14 Şuıbat 2019'da Yayınlanmıştır.

Дейл Петерсон
Dale Peterson
S4 Events Kurucusu ve Program Başkanı, Yazar, Konuşmacı, Podcast Üreticisi, ICS Güvenliği 94 Makale, Danışman (2000'den beri)

✓ Devam

https://www.linkedin.com/pulse/ics-security-patching-never-next-now-dale-peterson/

Teşekkürler!

SCADAfence

Value-Added Distributor
OTD BİLİŞİM
www.onlineteknikdestek.com

ICT
OTD
PREFER EXPERIENCE ONLINE
Since 2011