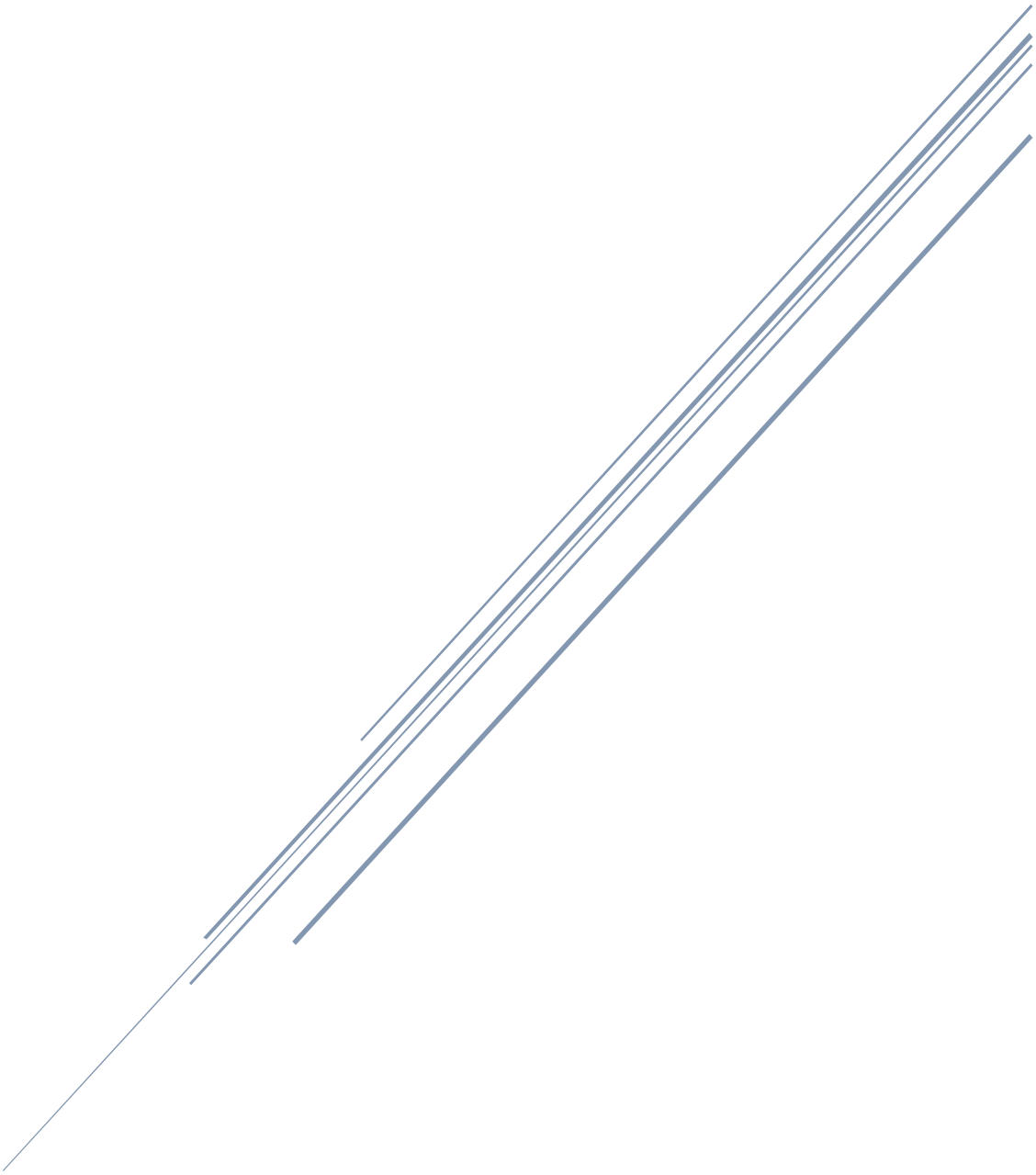
GRUP 1-2-4

NESSUS TARAMASI



TARAMALAR

42873 (1) - SSL Medium Strength Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/

https://sweet32.info

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

CVE CVE-2016-2183

Plugin Information

Published: 2009/11/23, Modified: 2021/02/03

Plugin Output

mustso.org.tr (tcp/443/www)

SSL NEDİR?

SSL internet ortamında çok karşılaşılan kavramlardan biridir. Genellikle alışveriş sitelerinde oldukça sık rastlanmaktadır. SSL'in açılımı **Secure Socket Layer**'dır. Türkçe anlamıysa **Güvenli Giriş Katmanı**'dır. SSL kişisel gizlilik ve güvenilirlik sağlayan, network üzerindeki bilgi transferi sırasında bilginin bütünlüğü ve gizliliği (*data protection*) için sunucu ile istemci arasındaki iletişimin şifrelenmiş şekilde yapılabilmesine imkan veren bu sayede gizliliğinin ve bütünlüğün korunmasını sağlayan **Netscape** tarafından geliştirilmiş bir güvenlik protokolüdür diye tanımlayabiliriz.

SSL protokolü bütün yaygın **web sunucuları** (server) ve **tarayıcıları** (browser) tarafından desteklenen bir protokoldür. SSL, standart bir algoritmadır. Milyonlarca web sitesinde güvenli veri iletişimi için kullanılmaktadır. SSL fonksiyonun çalışabilmesi için sunucu tarafında bir **anahtar** (private key) ve istemci tarafında çalışacak bir **sertifikaya** (Public Key) ihtiyaç duyulmaktadır.

SSL Nasıl Çalışır?

SSL Public Key/Private Key adı verilen anahtarların kullanımına bağlı bir kodlama yöntemine dayalıdır.

SSL kodlama için iki adet anahtar bulunmaktadır. Bu anahtarlar, dijital ortamda kodlanmış yazılımlardır. Bir anahtarın kilitlemiş olduğu veriyi, sadece diğer anahtar açabilir. Anahtarlarınızı yarattıktan sonra (SSL default olarak bu işlemi yapmaktadır, sizin herhangi bir işlem yapmanıza gerek yoktur), anahtarlardan biri (private key) sunucuda kalır. Diğer anahtar (public key) ise, bağlantı kurmak istediğiniz kişilere gönderilir.

Dışarıdan sizinle iletişime geçmek isteyen kişi, public key'i kullanarak mesajı güvenli bir şekilde size gönderir. Veri, size ulaşmadan, transfer sırasında veriye ulaşılsa bile, şifrenin çözülmesi için sizde bulunan private key gerekecektir.

ÇÖZÜM:

- Sistemde kullanılan SSL sertifikasına ait şifreleme algoritmasının anahtar uzayı bazı kriptoanaliz tekniklerine karşı yetersiz olduğu için, içeriden ağa bağlı bir saldırgana karşı güvenli değildir. Bunun çözüm yolu ise kullanılan şifreleme algoritmasının güncel kriptoanaliz yöntemlerine karşı güvenli olan şifreleme algoritmalarıyla değiştirilmesi gerekmektedir.
  Örnek; DHE, RSA, AES256, SHA256

- SSL sertifikasının sağladığı güvenlik yetersiz kaldığı durumlarda TLS 1.2v ve 1.3v protokolleri güvenlik seviyesini yükseltmek için kullanılabilir.

142960 (1) - HSTS Missing From HTTPS Server (RFC 6797)

Synopsis

The remote web server is not enforcing HSTS, as defined by RFC 6797.

Description

The remote web server is not enforcing HSTS, as defined by RFC 6797. HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2020/11/17, Modified: 2021/06/29

Plugin Output

mustso.org.tr (tcp/443/www)

```
The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

HTTP Katı Taşıma Güvenliği (HSTS) Nedir ?

web sitelerini protokol indirgeme ve oturum çalma saldırılarına karşı korumaya yardımcı olan bir web güvenlik politikası mekanizmasıdır. Web sunucuları, kendisine gönderilen isteklerin yalnızca HTTPS üzerinden olması gerektiğini web tarayıcılarına bu mekanizma ile belirtir. Bu sayede kullanıcı, herhangi bir güvenlik çözümü sunmayan HTTP yerine Taşıma Katmanı Güvenliği (TLS/SSL) sağlayan HTTPS kullanarak ilgili web sitesine erişim sağlar. HSTS, RFC 6797 ile detaylandırılan bir IETF Standards Track protokolüdür.

Sunucunun HSTS Politikası, yine sunucu tarafından HTTPS yanıt başlığındaki

Strict-Transport-Security alanı ile web tarayıcısına iletilir. HSTS politikası, tarayıcının sunucuya HTTPS kullanarak erişmesi gereken süreyi belirtir. HSTS kullanan web siteleri, HTTP üzerinden gelen bağlantıları reddederek veya kullanıcıları sistematik olarak HTTPS'ye yönlendirerek açık metin HTTP'yi kabul etmez (ancak bunun spesifikasyonda zorunlu olmadığı belirtilmiştir). Bunun sonucunda, TLS/SSL yapamayan web tarayıcısı bu siteye bağlanamayacaktır.

HSTS Eksik HTTPS Sunucu hatasının tehlikeleri nelerdir?

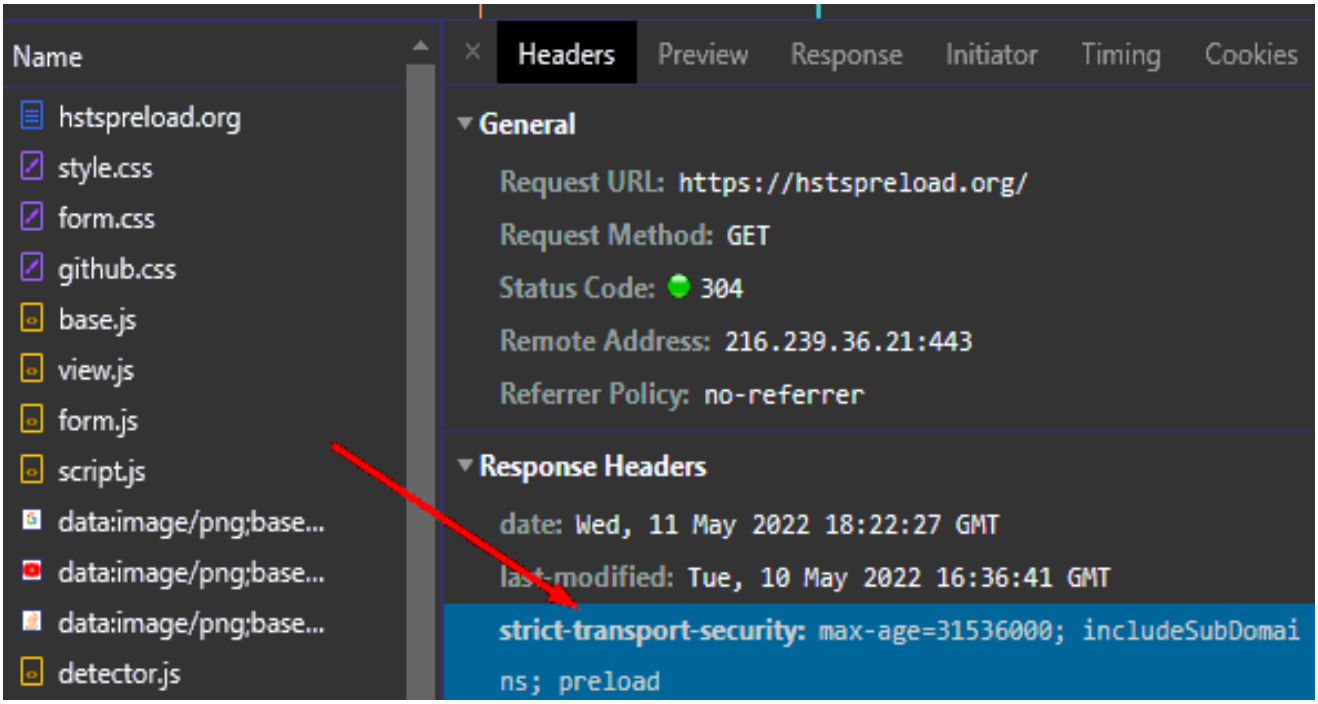
HSTS Eksik HTTPS Sunucu hatasının tehlikeleri aşağıda listelenmiştir.

- MITM: Ortadaki adam saldırıları, HSTS MISSING FROM HTTPS SERVER hatalarıyla mümkündür. Ve bir bilgisayar korsanı, bir kullanıcıyı bir HTTP URL'sinden bir klon web sitesine yönlendirebilir ve kullanıcıların bilgilerini kullanabilir.
- Çerez Ele Geçirme: Bir bilgisayar korsanı, bir HTTP bağlantısı aracılığıyla bir web sitesi oturumu sırasında çerezleri çalabilir. Ve bir çerez, kullanıcılar hakkında şifreler, kullanıcı adları ve diğer değerli özel bilgileri içerebilir.

Kendini HTTP'den HTTPS'ye yönlendiren bir web sitesi, bu tür eksik HSTS hata tehlikelerini engellemek için kesinlikle HSTS (HTTP Strict Transport Security) yanıt başlığını kullanmalıdır.

Saldırganlar neden HTTPS Sunucu Hatalarından Eksik HSTS'yi kullanıyor?

HTTPS Sunucusunda HSTS Eksikliği, web siteleri için orta riskli bir güvenlik açığıdır. Eksik HSTS, web sitesi bilgisayar korsanları ve saldırganlar için düşük asılı bir meyvedir. Düzeltmesi kolay olsa bile, sabitlenmemiş bir temel web güvenliği yanıt başlığı, HTTP Strict Transport Security gibi web kullanıcıları için büyük bir risk oluşturur. HSTS Yanıt Başlığı, bir web sitesini saldırganlardan korumak için yalnızca HTTPS bağlantısı tarafından kullanılmaya zorlar.



Eklenti Ayrıntıları

Önem : Orta
Kimlik : 142960
Dosya Adı : miss_hsts_rfc6797.nasl
Sürüm : 1.6
Tür : uzak
Aile : Web Sunucuları
yayınlandı : 17/11/2020
Güncellendi : 29.06.2021

Risk Bilgileri
CVSS Puan Rasyoneli : Satıcı tavsiyelerinin analizine dayalı puan.
CVSS v2
Risk Faktörü : Orta
Taban Puanı : 5.8
Vektör : AV:N/AC:M/Au:N/C:P/I:P/A:N
CVSS Puanı Kaynak : manuel
CVSS v3
Risk Faktörü : Orta
Temel Puan : 6.5
Vektör : CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

104743 (1) - TLS Version 1.0 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

Plugin Information

Published: 2017/11/22, Modified: 2020/03/31

Plugin Output

mustso.org.tr (tcp/443/www)

```
TLSv1 is enabled and the server supports at least one cipher.
```

157288 (1) - TLS Version 1.1 Protocol Deprecated

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticate encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://datatracker.ietf.org/doc/html/rfc8996

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

Plugin Information

Published: 2022/04/04, Modified: 2022/04/11

Plugin Output

mustso.org.tr (tcp/443/www)

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

121010 (1) - TLS Version 1.1 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

Plugin Information

Published: 2019/01/08, Modified: 2020/08/07

Plugin Output

mustso.org.tr (tcp/443/www)

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

TLS Nedir?

TLS (Transport Layer Security / Taşıma Katmanı Güvenliği), İnternet Mühendisliği Görev Gücü (IETF) standartlar yolu protokolüdür ve önceki SSL spesifikasyonları (1994, 1995, 1996) esas alınarak SSL'i de kullanıma sunan Netscape tarafından geliştirilmiştir. Bu açıdan değerlendirildiğinde, SSL için TLS'nin öncülü diyebiliriz. Bu nedenle kimi zaman SSL/TLS olarak da adlandırılır. Kısaca bu süreci açıklamak gerekirse, SSL protokolünün yayınlanan son versiyonu 3.0 sonrasında TLS 1.0 ile devamlılık sağlanmıştır. TLS 1.0'ın SSL 3.1'e karşılık geldiği düşünülebilir. Tabi eklenen özellikler ve modifiye edilen, daha gelişmiş ve güvenli hale getirilen yapı sebebiyle TLS ifadesi tercih edilmeye başlanmıştır.

TLS 1.0

TLS 1.0, bilgisayarların sahip olduğu ağlar üzerinden şifreleme için kullanılan kanalları kurmak adına tanımlanmış olan güvenlik protokolüdür. TLS 1.0, TLS'in ilk sürümüdür ve bundan dolayı birden fazla hata tespit edilmiştir ve zamanla yerini başka versiyonlara bırakmıştır.

Bundan dolayı TLS'in günümüzde kullandığımız yeni sürümlerinde TLS'in daha üst modelleri yer almaktadır.

Neden TLS 1.0 Kullanımdan Kaldırmamız Gerekiyor?

PCI DSS'in 3.1 ve 3.2 versiyonu ile birlikte, SSL v3.0 ve TLS v1.0 kullanımları artık güvensiz sayılmaktadır. SSL v3.0'da ve TLS v1.0'da çıkan POODLE, BEAST, CRIME adı verilen açıklar sebebi ile İstemci – sunucu arasına giren kötü niyetli bir kullanıcı aradaki bağlantı HTTPS bile olsa, içeriği okuyabilir, içeriği (bütünlüğü) değiştirebilir, hatta kriptografik anahtarlarınızı ele geçirebilir. SSL (ya da TLS), istemci ve sunucu arasındaki trafiği bir kriptografik anahtar ve sertifika kullanarak şifreliyor ve bu şekilde aradaki herhangi biri bu trafiği göremiyor.

TLS 1.1

Aktarım Katmanı Güvenliği (TLS), iki sistem arasında güvenli iletişim kanalı oluşturmak için kullanılan bir şifreleme protokolüdür. Sistemlerden birinin veya her ikisinin kimliğini doğrulamak ve aralarında paylaştıkları bilgilerin gizliliğini ve bütünlüğünü korumak için kullanılır. TLS 1.1 2006'da, bir sonraki sürüm olan TLS 1.2 2008'de ve en son sürüm olan TLS 1.3 2018'de kullanıma sunulmuştur.

Neden TLS 1.1 Kullanımdan Kaldırmamız Gerekiyor?

TLS 1.1 artık güvenli kabul edilmemektedir. Mart 2020 itibarıyla, başlıca web tarayıcılarının en son sürümleri TLS 1.1'i desteklememeye başladı. 2018'in ikinci yarısında Apple, Google, Microsoft ve Mozilla, 2020'nin başlarında TLS 1.1'i kullanımdan kaldırmayı planladıklarını açıkladılar.

Bilinen uygulanabilir saldırılara karşı şifreleme güvenliği

Şifreleme			Protokol versiyonu					Durum
Tip	Algoritma	Güç (bits)	SSL 2.0	SSL 3.0 [n 1][n 2][n 3][n 4]	TLS 1.0 [n 1][n 3]	TLS 1.1 [n 1]	TLS 1.2 [n 1]	
Block cipher mode of operation	AES GCM[n 5]	256, 128	Yok	Yok	Yok	Yok	Güvenli	RFC'lerde TLS 1.2 için tanımlanmıştır
	AES CCM[n 5]		Yok	Yok	Yok	Yok	Güvenli	
	AES CBC[n 6]		Yok	Yok	Alınan önlemlere göre değişir	Güvenli	Güvenli	
	Camellia GCM[n 5]	256, 128	Yok	Yok	Yok	Yok	Güvenli	
	Camellia CBC[n 6]		Yok	Yok	Alınan önlemlere göre değişir	Güvenli	Güvenli	
	ARIA GCM[n 5]	256, 128	Yok	Yok	Yok	Yok	Güvenli	
	ARIA CBC[n 6]		Yok	Yok	Alınan önlemlere göre değişir	Güvenli	Güvenli	
	SEED CBC[n 6]	128	Yok	Yok	Alınan önlemlere göre değişir	Güvenli	Güvenli	
	3DES EDE CBC[n 6]	112[n 7]	Güvensiz	Güvensiz	Az güçlü, Alınan önlemlere göre değişir	Az güçlü	Az güçlü	
	GOST 28147-89 CNT	256	Yok	Yok	Güvenli	Güvenli	Güvenli	RFC taslaklarında önerilmiştir
	IDEA CBC[n 6][n 8]	128	Güvensiz	Güvensiz	Depends on mitigations	Güvenli	Yok	TLS 1.2'den kaldırılmıştır
	DES CBC[n 6][n 8]	56	Güvensiz	Güvensiz	Güvensiz	Güvensiz	Yok	
		40	Güvensiz	Güvensiz	Güvensiz	Yok	Yok	TLS 1.1 ve sonrası için yasaklanmıştır
	RC2 CBC[n 6]	40	Güvensiz	Güvensiz	Güvensiz	Yok	Yok	
Stream cipher	ChaCha20-Poly1305[n 5]	256	Yok	Yok	Yok	Yok	Güvenli	RFC taslaklarında önerilmiştir
	RC4[n 9]	128	Güvensiz	Güvensiz	Güvensiz	Güvensiz	Güvensiz	TLS'nin tüm versiyonları için yasaklanmıştır
		40	Güvensiz	Güvensiz	Güvensiz	Yok	Yok	
None	**Null**[n 10]	-	Yok	Güvensiz	Güvensiz	Güvensiz	Güvensiz	RFC'lerde TLS 1.2 için tanımlanmıştır

Çözüm

TLS 1.0 ve 1.1'de bulunan açıklar sebebiyle versiyonun günümüzde daha güncel ve güvenilir olan versiyon 1.2 veya 1.3 versiyonuna yükseltilmesi gereklidir.

24260 (2) - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

mustso.org.tr (tcp/80/www)

```
Response Code : HTTP/1.1 301 Moved Permanently

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Content-Type: text/html; charset=UTF-8
  Location: https://www.mustso.org.tr/
  Server: Microsoft-IIS/8.5
  Date: Sat, 20 Aug 2022 12:50:14 GMT
  Content-Length: 149

Response Body :

<head><title>Document Moved</title></head>
<body><h1>Object Moved</h1>This document may be found <a HREF="https://www.mustso.org.tr/">here</
a></body>
```

mustso.org.tr (tcp/443/www)

```
Response Code : HTTP/1.1 301 Moved Permanently
```


.

HTTP İnformation

Bu test bize sadece bilgi verme amacını taşır. Bizlere http'nin hangi sürümün kullanıldığını, hangi özelliklere sahip olduğu (pipelining vs.) hakkında bilgi verir. Herhangi bir güvenlik sorununa işaret etmez

11936 (1) - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2022/03/09

Plugin Output

mustso.org.tr (tcp/0)

```
Remote operating system : Microsoft Windows Server 2012 R2
Confidence level : 75
Method : HTTP


The remote host is running Microsoft Windows Server 2012 R2
```

Uzak işletim sistemini tahmin etmek mümkündür. Uzak probların bir kombinasyonunu kullanarak (örneğin, TCP/IP, SMB, HTTP, NTP, SNMP, vb.), tahmin etmek mümkündür. Kullanılan uzak işletim sisteminin adını ve bazen versiyonu tahmin etmek de mümkündür.

İşletim sisteminin Windows server 2012 olduğu tespit edilmiştir.

İşletim sisteminin kesinlik oranı %75 olarak bulunmuştur.

46180 (1) - Additional DNS Hostnames

Synopsis

Nessus has detected potential virtual hosts.

Description

Hostnames different from the current hostname have been collected by miscellaneous plugins. Nessus has generated a list of hostnames that point to the remote host. Note that these are only the alternate hostnames for vhosts discovered on a web server.

Different web servers may be hosted on name-based virtual hosts.

See Also

https://en.wikipedia.org/wiki/Virtual_hosting

Solution

If you want to test them, re-scan using the special vhost syntax, such as :

www.example.com[192.0.32.10]

Risk Factor

None

Plugin Information

Published: 2010/04/29, Modified: 2022/08/15

Plugin Output

mustso.org.tr (tcp/0)

```
The following hostnames point to the remote host :
  - www.mustso.org.tr
```

Nessus potansiyel sanal host tespit etti. Mevcut ana bilgisayar adından farklı ana bilgisayar adlarına yönlendirme yapıyor olabilir. Nessus uzak ana bilgisayarı işaret eden bir ana bilgisayar adları listesi oluşturdu. Farklı web sunucuları, ad tabanlı sanal ana bilgisayarlarda barındırılabilir.

50845 (1) - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/11/30, Modified: 2020/06/12

Plugin Output

mustso.org.tr (tcp/443/www)

Sitenin SSL sertifikası olarak OpenSSL tercih edilmiştir. OpenSSL cPanel içerisinde ücretsiz olarak bulunan bir sertifika servisidir.

83298 (1) - SSL Certificate Chain Contains Certificates Expiring Soon

Synopsis

The remote host has an SSL certificate chain with one or more certificates that are going to expire soon.

Description

The remote host has an SSL certificate chain with one or more SSL certificates that are going to expire soon. Failure to renew these certificates before the expiration date may result in denial of service for users.

Solution

Renew any soon to expire SSL certificates.

Risk Factor

None

Plugin Information

Published: 2015/05/08, Modified: 2015/05/08

Plugin Output

mustso.org.tr (tcp/443/www)

```
The following soon to expire certificate was part of the certificate
chain sent by the remote host :

|-Subject   : CN=www.mustso.org.tr
|-Not After : Sep 05 10:36:26 2022 GMT
```

Site, yakında sona erecek bir veya daha fazla sertifikaya sahip bir SSL sertifika zincirine sahiptir.

Bu sertifikaların sona erme tarihinden önce yenilenmemesi, kullanıcılar için hizmet reddine neden olabilir.

EKİBİMİZ

github.com/bugracaydam / Buğra Çaydam
github.com/muhammetcg / Muhammet Can Görücü
github.com/smyyyaydn / Sümeyye Aydın
github.com/melihaarslan / Meliha Arslan
github.com/afur01 / Ahmet Furkan Bozkurt
github.com/cedogan / Ece Doğan
github.com/cvkmert / Mert Çevik
github.com/Abdullahgnan / Abdullah Günan
github.com/bedirhantuncer / Bedirhan Tuncer
github.com/onurcan-guler / Onurcan Güler
github.com/KaplanArdaUcar / Kaplan Arda Uçar

PUANLAMA

Buğra Çaydam ➔ **94**
Muhammet Can Görücü ➔ **86**
Sümeyye Aydın ➔ **91**
Meliha Arslan ➔ **97**
Ahmet Furkan Bozkurt ➔ **87**
Ece Doğan ➔ **86**
Mert Çevik ➔ **85**
Abdullah Günan ➔ **94**
Bedirhan Tuncer ➔ **92**
Onurcan Güler ➔ **85**
Kaplan Arda Uçar ➔ **89**