

Ποιές εκδόσεις TLS είναι συμβατές με το λογισμικό ή το λειτουργικό σύστημα που χρησιμοποιώ;

Ioanna Anifanti - 2022-12-17 - Email

Το Secure Socket Layer (SSL) και το Transport Layer Security (TLS) είναι και τα δύο πρωτόκολλα ισχυρής κρυπτογράφησης που παρέχουν ασφάλεια στην επικοινωνία σε ένα δίκτυο. Δίκτυο εννοούμε για παράδειγμα, όταν ένας client συνδέεται με ένα web server.

Τα συγκεκριμένα πρωτόκολλα χρησιμοποιούνται στην καθημερινότητά μας σε πλήθος εφαρμογών όπως στην περιήγηση μας στον παγκόσμιο ιστό, την υπηρεσία email, την μεταφορά αρχείων, την ανταλλαγή άμεσων μηνυμάτων, σε τηλεδιασκέψεις, VoIP κτλ. Το TLS είναι η συνέχεια του SSL πρωτοκόλλου.

Κατά το ξεκίνημα μιας TLS ή SSL σύνδεσης, πραγματοποιείται μια "χειραψία" (handshake) μεταξύ του client και του server, οι οποίοι θα ελέγξουν ποιοι είναι οι κοινοί αλγόριθμοι και πρωτόκολλα κρυπτογράφησης που υποστηρίζουν, ώστε να συνάψουν τη χειραψία με βάση αυτά και να καταφέρουν τελικά επικοινωνήσουν μεταξύ τους.

Με την πάροδο του χρόνου ωστόσο, ανακαλύπτονται νέες επιθέσεις εναντίον των πρωτοκόλλων SSL και TLS, για αυτό εκδίδονται νεότερες εκδόσεις, ώστε να καλύπτουν τα κενά ασφαλείας που εντοπίζονται. Αυτή τη στιγμή βρισκόμαστε στις εκδόσεις TLS v1.2 και TLS v1.3. Η χρήση παρωχημένων εκδόσεων του TLS, όπως η v1.0 και v1.1, οδηγεί σε αυξημένο κίνδυνο εκμετάλλευσης των ευπαθειών του πρωτοκόλλου από κακόβουλους χρήστες.

Για τους παραπάνω λόγους, οι εκδόσεις του πρωτοκόλλου TLS v1.0 και TLS v1.1, από τις 31/03/2021 κι έπειτα δεν θα υποστηρίζονται από την υποδομή μας.

Συνεπώς, πλατφόρμες λογισμικού και λειτουργικά συστήματα που είναι συμβατά μόνο με τις εκδόσεις του πρωτοκόλλου TLS v1.0 ή/και TLS v1.1, δεν θα μπορούν να συνάψουν "χειραψία" με τους servers της υποδομής μας, που σημαίνει πως δεν θα μπορούν να συνδεθούν και να επικοινωνήσουν μεταξύ τους.

Παρακάτω μπορείτε να δείτε τα πρωτόκολλα **TLS v1.0, v1.1, v1.2, & v1.3** και τη συμβατότητά τους με διάφορες πλατφόρμες λογισμικού και λειτουργικά συστήματα, τόσο από πλευράς client όσο και από πλευράς server.

| Browsers | TLS 1.0 | TLS 1.1 | TLS 1.2 | TLS 1.3 |
|---|----------------|-------------------------|-------------------------|----------------|
| Mobile IE v10 και χαμηλότερη | Ναι | Όχι | Όχι | Όχι |
| Desktop IE v7 και χαμηλότερη | Ναι | Όχι | Όχι | Όχι |
| Desktop IE v8, v9, και v10 | Ναι | Μερικώς (Σημείωση 1) | Μερικώς (Σημείωση 1) | Όχι |
| Desktop και mobile IE v11 | Ναι | Ναι | Ναι | Όχι |
| Microsoft Edge | Ναι | Ναι | Ναι | Όχι |
| Mozilla Firefox 22 και κάτω | Ναι | Όχι | Όχι | Όχι |
| Mozilla Firefox 23 έως 26 | Ναι | Μερικώς (Σημείωση 2) | Μερικώς (Σημείωση 2) | Όχι |
| Mozilla Firefox 27 και πάνω | Ναι | Ναι | Ναι | Όχι |
| Google Chrome 21 και κάτω | Ναι | Όχι | Όχι | Όχι |
| Google Chrome 22 έως 37 | Ναι | Μερικώς (Σημείωση 3) | Μερικώς (Σημείωση 3) | Όχι |
| Google Chrome 38 και πάνω | Ναι | Ναι | Ναι | Όχι |
| Android 4.3 (Jelly Bean) και κάτω | Ναι | Όχι | Όχι | Όχι |
| Android 4.4 (Kitkat) έως 4.4.4 | Ναι | Μερικώς (Σημείωση 4) | Μερικώς (Σημείωση 4) | Όχι |
| Android 5.0 (Lollipop) και πάνω | Ναι | Ναι | Ναι | Όχι |
| Mobile Safari για iOS 4 και κάτω | Ναι | Όχι | Όχι | Όχι |
| Mobile Safari v5 και υψηλότερη για iOS 5 και πάνω | Ναι | Ναι | Ναι | Όχι |
| Desktop Safari v6 και χαμηλότερη για OS X 10.8 (Mountain Lion) και κάτω | Ναι | Όχι | Όχι | Όχι |
| Desktop Safari v7 και υψηλότερη για OS X 10.9 (Mavericks) και πάνω | Ναι | Ναι | Ναι | Όχι |

| Desktop Clients | TLS 1.0 | TLS 1.1 | TLS 1.2 | TLS 1.3 |
|------------------------|----------------|-------------------------|-------------------------|----------------|
| Windows XP | Ναι | Όχι | Όχι | Όχι |
| Windows XP SP3 | Ναι | Ναι | Όχι | Όχι |
| Windows Vista | Ναι | Όχι | Όχι | Όχι |
| Windows 7 SP1 | Ναι | Ναι | Ναι | Όχι |
| Windows 8 | Ναι | Μερικώς (Σημείωση 5) | Μερικώς (Σημείωση 5) | Όχι |
| Windows 8.1 | Ναι | Ναι | Ναι | Όχι |
| Windows 10 | Ναι | Ναι | Ναι | Όχι |
| MAC OS X 10.2 και 10.3 | Ναι | Όχι | Όχι | Όχι |
| MAC OS X 10.4 και 10.5 | Ναι | Όχι | Όχι | Όχι |
| MAC OS X 10.6 και 10.7 | Ναι | Όχι | Όχι | Όχι |
| MAC OS X 10.8 | Ναι | Όχι | Όχι | Όχι |
| MAC OS X 10.9 | Ναι | Ναι | Ναι | Όχι |
| MAC OS X 10.10 | Ναι | Ναι | Ναι | Όχι |
| MAC OS X 10.11 | Ναι | Ναι | Ναι | Όχι |
| MAC OS X 10.12 | Ναι | Ναι | Ναι | Όχι |
| MAC OS X 10.13 | Ναι | Ναι | Ναι | Όχι |
| Linux | Ναι | Ναι | Ναι | Ναι |

Παρακαλώ σημειώστε ότι η συμβατότητα των Email Clients με το πρωτόκολλο TLS 1.2, σχετίζεται άμεσα με την συμβατότητα του λειτουργικού συστήματος του υπολογιστή σας με το πρωτόκολλο αυτό.

Email Clients & Desktop OS**TLS 1.2**

| | |
|--|-----|
| Outlook 2003 / Win XP (up to SP3) | Όχι |
| Outlook 2003 / Vista | Όχι |
| Outlook 2003 / Win7 | Όχι |
| Outlook 2003 / Win8+ | Ναι |
| Outlook 2007 / Win XP (up to SP3) | Όχι |
| Outlook 2007 / Vista | Όχι |
| Outlook 2007 / Win7 | Όχι |
| Outlook 2007 / Win8+ | Ναι |
| Outlook 2010 / Win XP SP3 | Όχι |
| Outlook 2010 / Vista | Όχι |
| Outlook 2010 / Win7 | Όχι |
| Outlook 2010 / Win8+ | Ναι |
| Outlook 2013 / Win7 | Όχι |
| Outlook 2013 / Win8+ | Ναι |
| Outlook 2016 / Win7 | Όχι |
| Outlook 2016 / Win8+ | Ναι |
| Outlook 2011 / Mac OSX 10.11-10.13 | Όχι |
| Outlook 2016 / Mac OSX 10.11-10.13 | Ναι |
| Mac Mail / Mac OSX 10.11 (El Capitan) | Όχι |
| Mac Mail / Mac OSX 10.12+ | Ναι |
| Mail / iOS 11+ | Ναι |
| Mail / Android 5+ | Ναι |
| Thunderbird 24.2 / Win XP+ or Mac 10.11+ | Όχι |
| Thunderbird 45.6 / Win XP+ or Mac 10.11+ | Ναι |
| Thunderbird 52.8 / Win XP+ or Mac 10.11+ | Ναι |

| Mobile Clients | TLS 1.0 | TLS 1.1 | TLS 1.2 | TLS 1.3 |
|--|---------|---------|---------|---------|
| Airwatch | Ναι | Ναι | Μερικώς | Όχι |
| Android v1.0 έως v4.4.4 | Ναι | Όχι | Όχι | Όχι |
| Android v5.0 έως v8.1 και Android P | Ναι | Ναι | Ναι | Όχι |
| iPhone OS v1, v2, v3, και v4 | Ναι | Όχι | Όχι | Όχι |
| iPhone OS v5, v6, v7, v8, v9, v10, και v11 | Ναι | Ναι | Ναι | Όχι |
| MobileIron Core v9.4 και χαμηλότερη | Ναι | Όχι | Όχι | Όχι |
| MobileIron Core v9.5 και υψηλότερη | Ναι | Ναι | Ναι | Όχι |
| MobileIron Cloud | Ναι | Ναι | Ναι | Όχι |
| Windows Phone v7, v7.5, v7.8 και v8 | Ναι | Όχι | Όχι | Όχι |
| Windows Phone v8.1 | Ναι | Ναι | Ναι | Όχι |
| Windows 10 Mobile v1511, v1607, v1703, και v1709 | Ναι | Ναι | Ναι | Όχι |

Σημείωση 1: Τα desktop IE v8, v9, και v10, είναι συμβατά με TLS 1.1 και TLS 1.2 μόνο όταν εκτελούνται σε Windows 7 ή νεότερα, αλλά by default είναι απενεργοποιημένα. Για να τα ενεργοποιήσετε το TLS 1.2 μπορείτε να δείτε [εδώ](#) περισσότερες λεπτομέρειες.

Σημείωση 2: Για το Firefox 23 έως 26 χρησιμοποιήστε about: config για να ενεργοποιήσετε το TLS 1.2, ενημερώνοντας την τιμή config.tls.version.max σε 3 για TLS 1.2.

Σημείωση 3: Για το Google Chrome 22 έως 37, το TLS 1.2 είναι συμβατό όταν εκτελείται σε Windows XP SP3, Vista ή νεότερα (desktop), OS X 10.6 (Snow Leopard) ή νεότερο (desktop) ή Android 2.3 (Gingerbread) ή νεότερο (mobile).

Σημείωση 4: Για Android 4.4, ενδέχεται να είναι συμβατό με TLS 1.2, αλλά ορισμένες συσκευές με Android 4.4.x ενδέχεται να μην υποστηρίζουν TLS 1.2 ή νεότερη έκδοση.

Σημείωση 5: Για τα Windows 8, το TLS 1.2 μπορεί να ενεργοποιηθεί ακολουθώντας τις οδηγίες που βρίσκονται [εδώ](#).

| Servers | TLS 1.0 | TLS 1.1 | TLS 1.2 | TLS 1.3 |
|--|---------|-------------------------|-------------------------|---------|
| Windows Server 2003 | Ναι | Όχι (Σημείωση 6) | Όχι (Σημείωση 6) | Όχι |
| Windows Server 2008 | Ναι | Όχι (Σημείωση 6) | Όχι (Σημείωση 6) | Όχι |
| Windows Server 2008 SP 2 με εγκατεστημένο windows update | Ναι | Ναι | Ναι | Όχι |
| Windows Server 2008 R2 | Ναι | Ναι | Ναι | Όχι |
| Windows Server 2012 | Ναι | Μερικώς (Σημείωση 7) | Μερικώς (Σημείωση 7) | Όχι |
| Windows Server 2012 R2 | Ναι | Ναι | Ναι | Όχι |
| Windows Server 2016 | Ναι | Ναι | Ναι | Όχι |

| Libraries | TLS 1.0 | TLS 1.1 | TLS 1.2 | TLS 1.3 |
|--------------------------------------|---------|-------------------------|-------------------------|---------|
| .NET 3.5 και κάτω | Ναι | Όχι | Όχι | Όχι |
| .NET 4.0 | Ναι | Ναι | Μερικώς (Σημείωση 9) | Όχι |
| .NET 4.5 έως 4.5.2 | Ναι | Μερικώς (Σημείωση 8) | Μερικώς (Σημείωση 8) | Όχι |
| .NET 4.6 και πάνω | Ναι | Ναι | Ναι | Όχι |
| OpenSSL v1.0.0 και χαμηλότερη | Ναι | Όχι | Όχι | Όχι |
| OpenSSL v1.0.1 και υψηλότερη | Ναι | Ναι | Ναι | Όχι |
| Mozilla - NSS v3.13.6 και χαμηλότερη | Ναι | Όχι | Όχι | Όχι |
| Mozilla - NSS v3.14 t έως v3.15 | Ναι | Ναι | Όχι | Όχι |
| Mozilla - NSS v3.15.1 και υψηλότερη | Ναι | Ναι | Ναι | Όχι |

Σημείωση 6: Ένας server που δεν υποστηρίζει TLS 1.2, ο οποίος συνδέεται σε άλλη τοποθεσία ως client, μπορεί να υποστηρίξει TLS 1.2 ενεργοποιώντας το μέσω των επιλογών Internet στο IE. Περιηγηθείτε στο Tools > Internet Options > Advanced. Στην ενότητα Security, θα δείτε τη λίστα των πρωτοκόλλων SSL που υποστηρίζονται από το IE. Επιλέξτε τα απαραίτητα boxes. Μπορείτε να δείτε [αυτό τον οδηγό](#) για περισσότερες πληροφορίες.

Σημείωση 7: Για Windows Server 2012, το TLS 1.2 μπορεί να ενεργοποιηθεί ακολουθώντας τις οδηγίες που βρίσκονται [εδώ](#).

Σημείωση 8: Για .NET 4.5 έως 4.5.2, το TLS 1.2 μπορεί να ενεργοποιηθεί ακολουθώντας μία από τις δύο επιλογές που αναφέρονται παρακάτω:

Επιλογή 1: Οι εφαρμογές .NET μπορούν να ενεργοποιήσουν απευθείας τα TLS 1.1 και TLS 1.2 μέσω του κώδικα λογισμικού τους ορίζοντας το System.Net.ServicePointManager.SecurityProtocol ώστε να ενεργοποιηθούν τα SecurityProtocolType.Tls12 και SecurityProtocolType.Tls11. Ο ακόλουθος C# κώδικας

είναι ένα παράδειγμα:

```
System.Net.ServicePointManager.SecurityProtocol = SecurityProtocolType.Tls12 |  
SecurityProtocolType.Tls11 | SecurityProtocolType.Tls;
```

Επιλογή 2: Για να ενεργοποιήσετε το TLS 1.2 by default (χωρίς να τροποποιήσετε τον πηγαίο κώδικα), μπορείτε να ορίσετε την τιμή του SchUseStrongCrypto DWORD στα ακόλουθα δύο registry keys σε 1, δημιουργώντας τα εάν δεν υπάρχουν:

```
"HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ .NETFramework \ v4.0.30319"
```

Και

```
"HKEY_LOCAL_MACHINE \ SOFTWARE \ Wow6432Node \ Microsoft \ .NETFramework \  
v4.0.30319". Παρόλο που η έκδοση των registry keys είναι 4.0.30319, τα .NET  
frameworks 4.5, 4.5.1 και 4.5.2 χρησιμοποιούν επίσης αυτές τις τιμές. Αυτά τα  
registry keys , ωστόσο, θα ενεργοποιήσουν το TLS 1.2 by default σε όλες τις  
εγκατεστημένες εφαρμογές .NET 4.0, 4.5, 4.5.1 και 4.5.2 σε αυτό το σύστημα.  
Συνιστάται να δοκιμάσετε αυτή την αλλαγή πριν την κάνετε deploy στους  
production servers.
```

Σημείωση 9: Για να ενεργοποιήσετε το TLS 1.2 by default, μπορείτε να εγκαταστήσετε το Framework .NET 4.5 ή νεότερη έκδοση και να ορίσετε την τιμή του SchUseStrongCrypto DWORD στα ακόλουθα δύο registry key σε 1, δημιουργώντας τα εάν δεν υπάρχουν:

```
"HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ .NETFramework \ v4.0.30319"
```

Και

```
"HKEY_LOCAL_MACHINE \ SOFTWARE \ Wow6432Node \ Microsoft \ .NETFramework \  
v4.0.30319". Αυτά τα registry keys, ωστόσο, ενδέχεται να ενεργοποιήσουν το TLS  
1.2 by default σε όλες τις εγκατεστημένες εφαρμογές .NET 4.0, 4.5, 4.5.1 και 4.5.2  
σε αυτό το σύστημα. Συνιστάται να δοκιμάσετε αυτή την αλλαγή πριν την κάνετε  
deploy στους production servers.
```

Σημείωση 10: Για την ενεργοποίηση του TLS 1.2 by default ως ασφαλές πρωτόκολλο στο WinHTTP(Windows HTTP Services) στα Windows, μπορείτε να δείτε τις οδηγίες που βρίσκονται [εδώ](#).

Σε περίπτωση που δεν είστε βέβαιοι ποια πρωτόκολλα υποστηρίζει ο server σας,

μπορείτε να χρησιμοποιήσετε [αυτόν τον checker](#), για να ελέγξετε γρήγορα τον server σας και να δείτε ποια πρωτόκολλα είναι ενεργοποιημένα.

Όπως αναφέρθηκε και παραπάνω, εφόσον για λόγους ασφαλείας, οι εκδόσεις του πρωτοκόλλου TLS v1.0 και TLS v1.1 από τις 31/03/2021 δεν θα υποστηρίζονται πλέον από την υποδομή μας, θα χρειαστεί να ελέγξετε εάν η εφαρμογή που χρησιμοποιείτε ή το λογισμικό σας είναι συμβατά και υποστηρίζουν τα πρωτόκολλα TLS v1.2, & v1.3.

Σε περίπτωση που έχετε κάποια εφαρμογή ή λογισμικό που υποστηρίζει μόνο τα πρωτόκολλα TLS v1.0 ή/και TLS v1.1, θα χρειαστεί να τα αναβαθμίσετε σε κάποια νεότερη έκδοση.