DOCUMENT – JANUARY 2023

PRINTED 27 JANUARY 2023

VMWARE VSPHERE 7 DEFAULT SSL/TLS CIPHER SUITES

VMwareSecurity

vmware®

Table of Contents

VMware vSphere 7 Default SSL/TLS Cipher Suites

Introduction

For many reasons, customers periodically enquire about which TLS cipher suites are supported by VMware vSphere. This resource outlines the default TLS settings, as detected experimentally with testssl.sh 3.0.1 using OpenSSL 1.0.2k-dev as delivered as part of that testssl.sh release ("testssl.sh -E host.name.com:443"). Ports & services using TLS were identified with nmap 7.70 ("nmap -p1-65535 -sT host.name.com") and verified with OpenSSL ("openssl s_client -connect host.name.com:443"). Products tested were in their default configurations with no additional hardening or configuration, against their configured management IP address, and with the Platform Services Controller functionality embedded in vCenter Server.

While we strive for accuracy this is not a comprehensive list of ports and protocols, nor a comprehensive list of ports that are TLS-enabled. Configurations and feature enablement differ between implementations, and enabling certain features will enable additional listening network ports. For descriptions of ports & protocols please use ports.vmware.com or refer to the product documentation. The sample commands above were given so that interested people may be able to replicate these tests in their own environment, and we encourage customers to take an active role in their security and compliance needs.

VMware vSphere 6.7 and newer default to only TLS 1.2. Earlier versions of vSphere have the "TLS Reconfiguration Utility" that can activate and deactivate TLS 1.0 and 1.1. Refer to the documentation for usage guidelines.

Activating and deactivating cipher suites is beyond the scope of this document and not recommended except under the direct guidance of VMware Global Support Services. As you see below, vSphere TLS 1.2 implementations do not contain ciphers known to be insecure (DES, RC4, etc.), or ciphers less than 128 bits, and meet all current regulatory & compliance framework requirements.

Requests for changes to cipher suite defaults are feature requests and should be done through your AE, SE, or TAM.

Disclaimer

This document is intended to provide general guidance for organizations that are considering VMware solutions. The information contained in this document is for educational and informational purposes only. This document is not intended to provide advice and is provided "AS IS." VMware makes no claims, promises, or guarantees about the accuracy, completeness, or adequacy of the information contained herein. Organizations should engage appropriate legal, business, technical, and audit expertise within their specific organization for review of requirements and effectiveness of implementations.

VMware vCenter Server 7.0

443/tcp:

```
TLS 1.2
 xc030    ECDHE-RSA-AES256-GCM-SHA384        ECDH 256   AESGCM      256
 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 xc028    ECDHE-RSA-AES256-SHA384            ECDH 256   AES         256
 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
 xc014    ECDHE-RSA-AES256-SHA               ECDH 256   AES         256
 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
 x9d      AES256-GCM-SHA384                  RSA        AESGCM      256      TLS_RSA_WITH_AES_256_GCM_SHA384

 x3d      AES256-SHA256                      RSA        AES         256      TLS_RSA_WITH_AES_256_CBC_SHA256

 x35      AES256-SHA                         RSA        AES         256      TLS_RSA_WITH_AES_256_CBC_SHA

 xc02f    ECDHE-RSA-AES128-GCM-SHA256        ECDH 256   AESGCM      128
 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 xc027    ECDHE-RSA-AES128-SHA256            ECDH 256   AES         128
 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
 xc013    ECDHE-RSA-AES128-SHA               ECDH 256   AES         128
```

```
 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
 x9c     AES128-GCM-SHA256                RSA        AESGCM      128      TLS_RSA_WITH_AES_128_GCM_SHA256

 x3c     AES128-SHA256                    RSA        AES         128      TLS_RSA_WITH_AES_128_CBC_SHA256

 x2f     AES128-SHA                       RSA        AES         128      TLS_RSA_WITH_AES_128_CBC_SHA
```

636/tcp:

```
TLS 1.2
 xc030   ECDHE-RSA-AES256-GCM-SHA384      ECDH 256   AESGCM      256
 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 xc028   ECDHE-RSA-AES256-SHA384          ECDH 256   AES         256
 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
 xc014   ECDHE-RSA-AES256-SHA             ECDH 256   AES         256
 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
 x9d     AES256-GCM-SHA384                RSA        AESGCM      256      TLS_RSA_WITH_AES_256_GCM_SHA384

 x3d     AES256-SHA256                    RSA        AES         256      TLS_RSA_WITH_AES_256_CBC_SHA256

 x35     AES256-SHA                       RSA        AES         256      TLS_RSA_WITH_AES_256_CBC_SHA

 xc02f   ECDHE-RSA-AES128-GCM-SHA256      ECDH 256   AESGCM      128
 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 xc027   ECDHE-RSA-AES128-SHA256          ECDH 256   AES         128
 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
 xc013   ECDHE-RSA-AES128-SHA             ECDH 256   AES         128
 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
 x9c     AES128-GCM-SHA256                RSA        AESGCM      128      TLS_RSA_WITH_AES_128_GCM_SHA256

 x3c     AES128-SHA256                    RSA        AES         128      TLS_RSA_WITH_AES_128_CBC_SHA256

 x2f     AES128-SHA                       RSA        AES         128      TLS_RSA_WITH_AES_128_CBC_SHA
```

1514/tcp:

```
TLS 1.2
 xc028   ECDHE-RSA-AES256-SHA384          ECDH 521   AES         256
 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
 xc014   ECDHE-RSA-AES256-SHA             ECDH 521   AES         256
 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
 x3d     AES256-SHA256                    RSA        AES         256      TLS_RSA_WITH_AES_256_CBC_SHA256

 x35     AES256-SHA                       RSA        AES         256      TLS_RSA_WITH_AES_256_CBC_SHA

 xc02f   ECDHE-RSA-AES128-GCM-SHA256      ECDH 521   AESGCM      128
 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 xc027   ECDHE-RSA-AES128-SHA256          ECDH 521   AES         128
 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
 xc013   ECDHE-RSA-AES128-SHA             ECDH 521   AES         128
 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
 x9c     AES128-GCM-SHA256                RSA        AESGCM      128      TLS_RSA_WITH_AES_128_GCM_SHA256

 x3c     AES128-SHA256                    RSA        AES         128      TLS_RSA_WITH_AES_128_CBC_SHA256

 x2f     AES128-SHA                       RSA        AES         128      TLS_RSA_WITH_AES_128_CBC_SHA
```

5480/tcp:

```
TLS 1.2
 xc030   ECDHE-RSA-AES256-GCM-SHA384      ECDH 256   AESGCM      256
```

```
 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 xc028   ECDHE-RSA-AES256-SHA384          ECDH 256   AES        256
 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
 xc014   ECDHE-RSA-AES256-SHA             ECDH 256   AES        256
 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
 x9d     AES256-GCM-SHA384                RSA        AESGCM     256      TLS_RSA_WITH_AES_256_GCM_SHA384

 x3d     AES256-SHA256                    RSA        AES        256      TLS_RSA_WITH_AES_256_CBC_SHA256

 x35     AES256-SHA                       RSA        AES        256      TLS_RSA_WITH_AES_256_CBC_SHA

 xc02f   ECDHE-RSA-AES128-GCM-SHA256      ECDH 256   AESGCM     128
 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 xc027   ECDHE-RSA-AES128-SHA256          ECDH 256   AES        128
 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
 xc013   ECDHE-RSA-AES128-SHA             ECDH 256   AES        128
 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
 x9c     AES128-GCM-SHA256                RSA        AESGCM     128      TLS_RSA_WITH_AES_128_GCM_SHA256

 x3c     AES128-SHA256                    RSA        AES        128      TLS_RSA_WITH_AES_128_CBC_SHA256

 x2f     AES128-SHA                       RSA        AES        128      TLS_RSA_WITH_AES_128_CBC_SHA
```

5580/tcp:

```
TLS 1.2
 xc030   ECDHE-RSA-AES256-GCM-SHA384      ECDH 256   AESGCM     256
 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 xc028   ECDHE-RSA-AES256-SHA384          ECDH 256   AES        256
 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
 xc014   ECDHE-RSA-AES256-SHA             ECDH 256   AES        256
 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
 x9d     AES256-GCM-SHA384                RSA        AESGCM     256      TLS_RSA_WITH_AES_256_GCM_SHA384

 x3d     AES256-SHA256                    RSA        AES        256      TLS_RSA_WITH_AES_256_CBC_SHA256

 x35     AES256-SHA                       RSA        AES        256      TLS_RSA_WITH_AES_256_CBC_SHA

 xc02f   ECDHE-RSA-AES128-GCM-SHA256      ECDH 256   AESGCM     128
 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 xc027   ECDHE-RSA-AES128-SHA256          ECDH 256   AES        128
 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
 xc013   ECDHE-RSA-AES128-SHA             ECDH 256   AES        128
 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
 x9c     AES128-GCM-SHA256                RSA        AESGCM     128      TLS_RSA_WITH_AES_128_GCM_SHA256

 x3c     AES128-SHA256                    RSA        AES        128      TLS_RSA_WITH_AES_128_CBC_SHA256

 x2f     AES128-SHA                       RSA        AES        128      TLS_RSA_WITH_AES_128_CBC_SHA
```

8084/tcp:

```
TLS 1.2
 xc030   ECDHE-RSA-AES256-GCM-SHA384      ECDH 256   AESGCM     256
 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 xc028   ECDHE-RSA-AES256-SHA384          ECDH 256   AES        256
 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
 xc014   ECDHE-RSA-AES256-SHA             ECDH 256   AES        256
 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
 x9d     AES256-GCM-SHA384                RSA        AESGCM     256      TLS_RSA_WITH_AES_256_GCM_SHA384
```

```
 x3d     AES256-SHA256                   RSA        AES        256      TLS_RSA_WITH_AES_256_CBC_SHA256

 x35     AES256-SHA                      RSA        AES        256      TLS_RSA_WITH_AES_256_CBC_SHA

 xc02f   ECDHE-RSA-AES128-GCM-SHA256     ECDH 256   AESGCM     128
 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 xc027   ECDHE-RSA-AES128-SHA256         ECDH 256   AES        128
 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
 xc013   ECDHE-RSA-AES128-SHA            ECDH 256   AES        128
 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
 x9c     AES128-GCM-SHA256               RSA        AESGCM     128      TLS_RSA_WITH_AES_128_GCM_SHA256

 x3c     AES128-SHA256                   RSA        AES        128      TLS_RSA_WITH_AES_128_CBC_SHA256

 x2f     AES128-SHA                      RSA        AES        128      TLS_RSA_WITH_AES_128_CBC_SHA
```

9087/tcp:

```
TLS 1.2
 xc030   ECDHE-RSA-AES256-GCM-SHA384     ECDH 521   AESGCM     256
 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 xc028   ECDHE-RSA-AES256-SHA384         ECDH 521   AES        256
 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
 xc014   ECDHE-RSA-AES256-SHA            ECDH 521   AES        256
 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
 x9d     AES256-GCM-SHA384               RSA        AESGCM     256      TLS_RSA_WITH_AES_256_GCM_SHA384

 x3d     AES256-SHA256                   RSA        AES        256      TLS_RSA_WITH_AES_256_CBC_SHA256

 x35     AES256-SHA                      RSA        AES        256      TLS_RSA_WITH_AES_256_CBC_SHA

 xc02f   ECDHE-RSA-AES128-GCM-SHA256     ECDH 521   AESGCM     128
 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 xc027   ECDHE-RSA-AES128-SHA256         ECDH 521   AES        128
 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
 xc013   ECDHE-RSA-AES128-SHA            ECDH 521   AES        128
 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
 x9c     AES128-GCM-SHA256               RSA        AESGCM     128      TLS_RSA_WITH_AES_128_GCM_SHA256

 x3c     AES128-SHA256                   RSA        AES        128      TLS_RSA_WITH_AES_128_CBC_SHA256

 x2f     AES128-SHA                      RSA        AES        128      TLS_RSA_WITH_AES_128_CBC_SHA
```

9443/tcp:

```
TLS 1.2
 xc030   ECDHE-RSA-AES256-GCM-SHA384     ECDH 521   AESGCM     256
 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 xc028   ECDHE-RSA-AES256-SHA384         ECDH 521   AES        256
 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
 xc014   ECDHE-RSA-AES256-SHA            ECDH 521   AES        256
 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
 x9d     AES256-GCM-SHA384               RSA        AESGCM     256      TLS_RSA_WITH_AES_256_GCM_SHA384

 x3d     AES256-SHA256                   RSA        AES        256      TLS_RSA_WITH_AES_256_CBC_SHA256

 x35     AES256-SHA                      RSA        AES        256      TLS_RSA_WITH_AES_256_CBC_SHA

 xc02f   ECDHE-RSA-AES128-GCM-SHA256     ECDH 521   AESGCM     128
 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 xc027   ECDHE-RSA-AES128-SHA256         ECDH 521   AES        128
```

```
 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
 xc013   ECDHE-RSA-AES128-SHA            ECDH 521   AES        128
 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
 x9c     AES128-GCM-SHA256               RSA        AESGCM     128      TLS_RSA_WITH_AES_128_GCM_SHA256

 x3c     AES128-SHA256                   RSA        AES        128      TLS_RSA_WITH_AES_128_CBC_SHA256

 x2f     AES128-SHA                      RSA        AES        128      TLS_RSA_WITH_AES_128_CBC_SHA
```

VMware ESXi 7.0

443/tcp:

```
TLS 1.2
 xc030   ECDHE-RSA-AES256-GCM-SHA384     ECDH 256   AESGCM     256
 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 xc028   ECDHE-RSA-AES256-SHA384         ECDH 256   AES        256
 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
 xc014   ECDHE-RSA-AES256-SHA            ECDH 256   AES        256
 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
 x9d     AES256-GCM-SHA384               RSA        AESGCM     256      TLS_RSA_WITH_AES_256_GCM_SHA384

 x3d     AES256-SHA256                   RSA        AES        256      TLS_RSA_WITH_AES_256_CBC_SHA256

 x35     AES256-SHA                      RSA        AES        256      TLS_RSA_WITH_AES_256_CBC_SHA

 xc02f   ECDHE-RSA-AES128-GCM-SHA256     ECDH 256   AESGCM     128
 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 xc027   ECDHE-RSA-AES128-SHA256         ECDH 256   AES        128
 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
 xc013   ECDHE-RSA-AES128-SHA            ECDH 256   AES        128
 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
 x9c     AES128-GCM-SHA256               RSA        AESGCM     128      TLS_RSA_WITH_AES_128_GCM_SHA256

 x3c     AES128-SHA256                   RSA        AES        128      TLS_RSA_WITH_AES_128_CBC_SHA256

 x2f     AES128-SHA                      RSA        AES        128      TLS_RSA_WITH_AES_128_CBC_SHA
```

9080/tcp:

```
TLS 1.2
 xc030   ECDHE-RSA-AES256-GCM-SHA384     ECDH 256   AESGCM     256
 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 xc028   ECDHE-RSA-AES256-SHA384         ECDH 256   AES        256
 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
 xc014   ECDHE-RSA-AES256-SHA            ECDH 256   AES        256
 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
 x9d     AES256-GCM-SHA384               RSA        AESGCM     256      TLS_RSA_WITH_AES_256_GCM_SHA384

 x3d     AES256-SHA256                   RSA        AES        256      TLS_RSA_WITH_AES_256_CBC_SHA256

 x35     AES256-SHA                      RSA        AES        256      TLS_RSA_WITH_AES_256_CBC_SHA

 xc02f   ECDHE-RSA-AES128-GCM-SHA256     ECDH 256   AESGCM     128
 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 xc027   ECDHE-RSA-AES128-SHA256         ECDH 256   AES        128
 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
 xc013   ECDHE-RSA-AES128-SHA            ECDH 256   AES        128
 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
 x9c     AES128-GCM-SHA256               RSA        AESGCM     128      TLS_RSA_WITH_AES_128_GCM_SHA256
```

x3c	AES128-SHA256	RSA	AES	128	TLS_RSA_WITH_AES_128_CBC_SHA256
x2f	AES128-SHA	RSA	AES	128	TLS_RSA_WITH_AES_128_CBC_SHA

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com