DOCUMENT – JANUARY 2023

PRINTED 27 JANUARY 2023

VMWARE VSPHERE 8 DEFAULT SSL/TLS CIPHER SUITES

VMwareCompliance

vmware®

Table of Contents

VMware vSphere 8 Default SSL/TLS Cipher Suites

Introduction

Customers periodically inquire about which TLS cipher suites are supported by VMware vSphere. This resource outlines the default TLS settings, as verified experimentally with testssl.sh 3.0.7 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.

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. It is also limited to ingress/incoming connections to vSphere. 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. 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. Unlike previous versions, **ESXi 8 cannot be downgraded to support TLS 1.0 or 1.1**.

Activating and deactivating particular ciphers is beyond the scope of this document and not recommended except under the direct guidance of VMware Global Support Services. Changes made by customers to cipher suites are not tested by VMware, may cause incompatibilities and system malfunctions, and may be inaccessible or overwritten during patching or updates. 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. We routinely suggest to organizations that the relative risk of the default cipher settings be assessed in context with the overall security of the environment when organizations decide how to spend their limited staff time in pursuit of better security.

Services that are meant to be internal to vSphere have had their cipher lists condensed as part of our ongoing effort to improve security and reduce attack surface while retaining compatibility with supported versions of vSphere. Other services have cipher suites that are chosen specifically to maximize security while retaining necessary compatibility with the larger infrastructure ecosystem. Speaking specifically, Microsoft Windows Server 2012 is prevalent in data centers and the ecosystem at large, is supported by Microsoft until October 10, 2023, and requires some backwards compatibility in the cipher suites in order to permit connections. While many TLS "best practices" guides often specify more limited sets of ciphers, real-world constraints and context always factor into deployments. As mentioned above, all of the ciphers included in vSphere 8 are considered to be secure at this time.

Requests for changes to cipher suite defaults are feature requests and should be done through your account team or Technical Account Manager (TAM). Thank you.

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 8.0

443/tcp:

TLS 1.2

```
xc030   ECDHE-RSA-AES256-GCM-SHA384     ECDH 256   AESGCM      256
TLS_ECDHE_RSA_WITH_AES_256_GCM_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
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
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
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

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

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
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
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
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
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 256   AESGCM      256
TLS_ECDHE_RSA_WITH_AES_256_GCM_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
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
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
x2f     AES128-SHA                      RSA        AES         128
TLS_RSA_WITH_AES_128_CBC_SHA
```

VMware ESXi 8.0

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
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
```

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
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
```

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