シスコ製品に影響する、SaltStack フレームワークの脆弱性

Critical

アドバイザリーID : cisco-sa-salt-2vx545AG

初公開日 : 2020-05-28 16:00

最終更新日 : 2020-06-16 15:17

バージョン 2.0 : Final

CVSSスコア : 10.0

回避策 : Yes

Cisco バグ ID : CSCvu43116 CSCvu33581

CVE-2020-11652

CVE-2020-11651

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

概要

2020 年 4 月 29日、ソルトオープンコアチームは、次の 2 つの CVE ID についてコミュニティに通知しました。

- CVE-2020-11651： 認証バイパスの脆弱性
- CVE-2020-11652： ディレクトリトラバーサルの脆弱性

Cisco Modeling Labs Corporate Edition（CML）、Cisco TelePresence IX5000 シリーズ、Cisco Virtual Internet Routing Lab Personal Edition（VIRL-PE）に組み込まれているバージョンの SaltStack では、これらの脆弱性の影響を受ける salt-master サービスが実行されています。

シスコはこれらの脆弱性に対処するソフトウェア アップデートを提供しています。 これらの脆弱性には、回避策が存在します。

このアドバイザリは、次のリンクより確認できます。
https://www.cisco.com/c/ja_jp/support/docs/csa/2020/cisco-sa-salt-2vx545AG.html

該当製品

脆弱性のある製品

これらの脆弱性は、脆弱なソフトウェアリリースを実行している場合、次のシスコ製品に影響

します。

- Modeling Labs Corporate Edition（CML）
- TelePresence IX5000 シリーズ
- Virtual Internet Routing Lab Personal Edition（VIRL-PE）

Cisco CML および Cisco VIRL-PE

Cisco CML と Cisco VIRL-PE は、スタンドアロン設定またはクラスタ設定のいずれかで展開できます。 この脆弱性は、展開ごとに異なる影響を与えます。 影響情報と推奨処置については、このアドバイザリの「詳細」の項にある表を参照してください。

注: シスコインフラストラクチャは、Cisco VIRL-PE で使用される salt-master サーバを維持します。 これらのサーバは、2020 年 5 月 7 日にアップグレードされました。 シスコは、Cisco VIRL-PE リリース 1.2 および 1.3 にサービスを提供している salt-master サーバが侵害されたことを確認しました。 サーバが 2020 年 5 月 7 日に修復されました。 次のサーバが侵害されました。

- us-1.virl.info
- us-2.virl.info
- us-3.virl.info
- us-4.virl.info
- vsm-us-1.virl.info
- vsm-us-2.virl.info

Cisco VIRL-PE は、salt-master サービスを実行しているシスコが管理する Salt サーバに接続します。 これらのサーバは、実行されている Cisco VIRL-PE ソフトウェアのリリースに応じて、異なる Cisco salt-master サーバと通信するように設定されています。 管理者は、[VIRL サーバ（VIRL Server）] > [Salt 設定とステータス（Salt Configuration and Status）] の順に移動して、設定済みの Cisco salt-master サーバを確認できます。

Cisco CML は、シスコによって管理されている Salt サーバに接続しません。

Cisco TelePresence IX5000 シリーズ

Cisco TelePresence IX5000 シリーズでは、ソルトサービスがデフォルトで有効です。

脆弱性を含んでいないことが確認された製品

このアドバイザリの脆弱性のある製品セクションに記載されている製品のみが、これらの脆弱性の影響を受けることが分かっています。

詳細

Cisco CML および Cisco VIRL-PE

Cisco CML と Cisco VIRL-PE の詳細については、「Cisco Modeling Labs」を参照してください。

Cisco CML および Cisco VIRL-PE ソフトウェアリリース 1.5 および 1.6 の場合、salt-master サービスが有効になっている場合、展開方法によって、製品がエクスプロイトされる可能性が左右されます。 攻撃を受けるには、salt-master サービスが TCP ポート 4505 および 4506 で到達可能である必要があります。 salt-master サービスが実行されているインストール環境ではマシンの侵害を検査するか、マシンを再イメージ化して、最新バージョンの Cisco CML または Cisco VIRL-PE をインストールすることを推奨します。

Cisco CML と Cisco VIRL-PE のインストール時に salt-master サービスのステータスを確認するには、デバイスにログインして、 **sudo systemctl status salt-master コマンドを実行します。** 「Active: active (running)」で示されているように、salt-master サービスがアクティブな場合は、次のようになります。 デバイスは脆弱になるため、次の表に記載されているアクションに従うことをお勧めします。

次の例は、salt-master サービスが有効になっているデバイスを示しています。

```
virl@virl:~$ sudo systemctl status salt-master
? salt-master.service - The Salt Master Server
   Loaded: loaded (/lib/systemd/system/salt-master.service; disabled; vendor preset: enabled)
  Drop-In: /etc/systemd/system/salt-master.service.d
           +-override.conf
   Active: active (running) since Thu 2020-05-28 17:55:10 GMT; 1s ago
     Docs: man:salt-master(1)
           file:///usr/share/doc/salt/html/contents.html
           https://docs.saltstack.com/en/latest/contents.html
 Main PID: 20662 (/usr/bin/python)
    Tasks: 16
   Memory: 217.9M
      CPU: 7.870s
   CGroup: /system.slice/salt-master.service
           +-20662 /usr/bin/python /usr/bin/salt-master ProcessManage
           +-20789 /usr/bin/python /usr/bin/salt-master MultiprocessingLoggingQueu
           +-20793 /usr/bin/python /usr/bin/salt-master ZeroMQPubServerChanne
           +-20794 /usr/bin/python /usr/bin/salt-master EventPublishe
           +-20797 /usr/bin/python /usr/bin/salt-master Maintenanc
           +-20798 /usr/bin/python /usr/bin/salt-master ReqServer_ProcessManage
           +-20799 /usr/bin/python /usr/bin/salt-master MWorkerQueu
           +-20804 /usr/bin/python /usr/bin/salt-master MWorker-
           +-20805 /usr/bin/python /usr/bin/salt-master MWorker-
           +-20806 /usr/bin/python /usr/bin/salt-master MWorker-May 28 17:55:08 virl systemd[1]: Starting
The Salt Master Server...
May 28 17:55:10 virl systemd[1]: Started The Salt Master Server.
virl@virl:~$
```

次の例は、salt-master サービスが有効にされていないデバイスです。

```
virl@virl:~$ sudo systemctl status salt-master
? salt-master.service - The Salt Master Server
```

```
  Loaded: loaded (/lib/systemd/system/salt-master.service; disabled; vendor preset: enabled)
 Drop-In: /etc/systemd/system/salt-master.service.d
          +-override.conf
  Active: inactive (dead)
    Docs: man:salt-master(1)
          file:///usr/share/doc/salt/html/contents.html
          https://docs.saltstack.com/en/latest/contents.html
```

次の表では、各シスコソフトウェアリリースの各展開オプションの影響と推奨処置を示しています。

Cisco CML および VIRL-PE ソフトウェアリリース	導入オプション	影響	推奨処置
2.0	スタンドアロン	影響なし。 Salt サービスを実行しません。	ありません。
2.0	クラスタ モード	影響なし。 現在、サポートされていません。	ありません。
1.6	スタンドアロン	新規インストールを実行したお客様には影響はありません。 インストールでは、必要な場合にのみ salt-minion プロセスが実行されます。 salt-master サービスは実行されません。 リリース 1.5 からアップグレードしたお客様の場合は、salt-master サービスが実行されています。	**sudo systemctl status salt-master** コマンドを使用して、salt-master サービスのステータスを確認してください。 salt-master サービスが実行されている場合は、次のいずれかを実行します。 • salt-master サービスを無効にするパッチリリースにアップグレードします。1 • 回避策を使用して、salt-master サービスを無効にします。
1.6	クラスタ モード	新規インストールを実行したお客様には影響はありません。 コントローラは SaltStack マスターを実行し、コンピューティングノードと通信します。 SaltStack マスターはプライベートネットワークにのみバインドされます。 リリース 1.5 からアップグレードしたお客様の場合は、salt-master サービスが実行されています。	**sudo systemctl status salt-master** コマンドを使用して、salt-master サービスのステータスを確認してください。 salt-master サービスが実行されている場合は、次のいずれかを実行します。 • パッチリリースへのアップグレードにより、内部（INT）ネットワークを除くすべてのインターフェース上の salt-master サ

			ービスが無効になります。1
1.5	スタンドアロン	salt-minion サービスが実行されています。 salt-master サービスが実行されています（すべてのインターフェイスにバインドされている）。 **注:** Salt サービスが CML で実行されていません。	**sudo systemctl status salt-master** コマンドを使用して、salt-master サービスのステータスを確認してください。 salt-master サービスが実行されている場合は、次のいずれかを実行します。 • salt-master サービスを無効にするパッチリリースにアップグレードします。1 • 回避策を使用して、salt-master サービスを無効にします。
1.5	クラスタ モード	salt-minion サービスが実行されています。 salt-master サービスが実行されています（すべてのインターフェイスにバインドされている）。	パッチリリースへのアップグレードにより、内部（INT）ネットワークを除くすべてのインターフェース上の salt-master サービスが無効になります。1
1.3	スタンドアロン	salt-minion サービスが実行されています。 salt-master サービスが実行されています（すべてのインターフェイスにバインドされている）。	**CML** 次のいずれかを実行します。 • salt-master サービスを無効にするパッチリリースにアップグレードします。1 • 回避策を使用して、salt-master サービスを無効にします。 **VIRL-PE** マシンのイメージを再作成し、VIRL-PE パッチリリースをインストールします。1
1.3	クラスタ モード	salt-minion サービスが実行されています。 salt-master サービスが実行されています（すべてのインターフェイスにバインドされてい	**CML** パッチリリースに移行します。1 **VIRL-PE** マシンのイメージを再作成し、VIRL-PE パッ

		る ）。	チリリースをインストールします。1
1.2	スタンドアロン	salt-minion サービスが実行されています。 salt-master サービスが実行されています（すべてのインターフェイスにバインドされている ）。	**CML** 次のいずれかを実行します。 • salt-master サービスを無効にするパッチリリースにアップグレードします。1 • 回避策を使用して、salt-master サービスを無効にします。 **VIRL-PE** マシンのイメージを再作成し、VIRL-PE パッチリリースをインストールします。1
1.2	クラスタ モード	salt-minion サービスが実行されています。 salt-master サービスが実行されています（すべてのインターフェイスにバインドされている ）。	**CML** パッチリリースに移行します。1 **VIRL-PE** マシンのイメージを再作成し、VIRL-PE パッチリリースをインストールします。1

1. 推奨するパッチリリースについては、このアドバイザリの「修正済みソフトウェア」のセクションを参照してください。

Cisco TelePresence IX5000 シリーズ

Cisco TelePresence IX5000 ではソルトサービスがデフォルトで有効ですが、これらのサービスは通常の操作では必要ありません。 サービスを無効にする方法については、「 回避策」セクションを参照してください。

回避策

Cisco CML および Cisco VIRL-PE

Cisco CML および Cisco VIRL-PE ソフトウェアリリース 2.0 以降では、salt-master サービスは実行されません。

スタンドアロンモードで展開された Cisco CML および Cisco VIRL-PE の場合、次の例に示すように、管理者は salt-master サービスのステータスを確認し、サービスを無効にできます。

```
virl@virl:~$ sudo systemctl status salt-master
? salt-master.service - The Salt Master Server
   Loaded: loaded (/lib/systemd/system/salt-master.service; disabled; vendor preset: enabled)
  Drop-In: /etc/systemd/system/salt-master.service.d
           +-override.conf
   Active: active (running) since Thu 2020-05-28 17:55:10 GMT; 1s ago
     Docs: man:salt-master(1)
           file:///usr/share/doc/salt/html/contents.html
           https://docs.saltstack.com/en/latest/contents.html

--- Output Omitted ---

virl@virl:~$ sudo systemctl stop salt-master
virl@virl:~$ sudo systemctl disable salt-master
Synchronizing state of salt-master.service with SysV init with /lib/systemd/systemd-sysv-install...
Executing /lib/systemd/systemd-sysv-install disable salt-master
insserv: warning: current start runlevel(s) (empty) of script `salt-master' overrides LSB defaults (2 3 4
5).
insserv: warning: current stop runlevel(s) (0 1 2 3 4 5 6) of script `salt-master' overrides LSB defaults (0
1 6).
virl@virl:~$
```

クラスタモードで展開された Cisco CML および Cisco VIRL-PE の場合、管理者は salt-master サービスのステータスを確認し、すべてのコンピューティングノードでサービスを無効にすることができます。 スタンドアロン展開については、上記の手順に従ってください。 次の例に示すように、クラスタコントローラノードでは、salt-master がクラスタ間通信のプライベート ネットワーク インターフェイスでのみリッスンしていることを確認します。

```
virl@virl:~$ netstat -tulpn | grep 450
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
tcp        0      0 172.16.10.250:4505      0.0.0.0:*               LISTEN      -
tcp        0      0 172.16.10.250:4506      0.0.0.0:*               LISTEN      -
virl@virl:~$
```

次の例に示すように、salt-master がすべてのインターフェイスをリッスンしている場合、お客様はパッチリリースにアップグレードする必要があります。

```
virl@virl:~$ netstat -tulpn | grep 450
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
tcp        0      0 0.0.0.0:4505      0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:4506      0.0.0.0:*               LISTEN      -
virl@virl:~$
```

Cisco TelePresence IX5000 シリーズ

Cisco TelePresence IX5000 シリーズでソルトサービスを完全に無効にするには、起動スクリプトファイルに変更を加える必要があります。これにはデバイスへの*ルートアクセス*が必要です。サポートについては、サポート組織を通して Cisco TAC にお問い合わせください。

修正済みソフトウェア

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェア アップデートを提供しています。 お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。 そのようなソフトウェア アップグレードをインストール、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、お客様は以下のリンクに記載されたシスコのソフトウェア ライセンスの条項に従うことに同意したことになります。 https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。 通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。 無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

ソフトウェアのアップグレードを検討する際には、Cisco Security Advisories and Alerts ページで入手できるシスコ製品のアドバイザリを定期的に参照して、侵害を受ける可能性と完全なアップグレード ソリューションを確認してください。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成は新規リリースでも継続して適切なサポートが受けられることを確認してください。 不明な点については、Cisco Technical Assistance Center (TAC) もしくは契約しているメンテナンス プロバイダーにお問い合わせください。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティ ベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco TAC に連絡してアップグレードを入手してください。
https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

修正済みリリース

Cisco CML

スタンドアロン展開でソフトウェアを実行しているお客様は、Cisco CML リリース 2.0 に移行することをお勧めします。

Cisco.com の Software Center からソフトウェアをダウンロードするには、次の手順を実行します。

1. [すべて参照（Browse all）] をクリックします。
2. [クラウドおよびシステム管理（Cloud and Systems Management）] **> [ネットワークモデリング（Network Modeling）] > [Modeling Labs]** を選択します。
3. 左側のペインからリリースを選択します。

リリース 2.0 に移行できないお客様は、リリース1.6.67 に移行することを推奨します。

Cisco CML は、Cisco CML 1.x リリースのインプレースアップグレードをサポートしていません。 お客様には、新しい Cisco CML リリース 1.6.67 または リリース 2.0 のインストールに移行することを推奨します。

シスコでは、Cisco CML リリース1.6.67 でこの脆弱性を修正しました。 このリリースでは、両方の脆弱性の修正を含む SaltStack のバージョンにアップグレードされます。 プライベート インターフェイスでのみソルトサービスが有効な Cisco CML リリース 1.6.65 を実行しているお客様も、リリース 1.6.67 に移行することが推奨されます。

Cisco 型 I PE

シスコは、Cisco Modeling Labs-Personal にブランド変更された Cisco VIRL-PE リリース 2.0 への移行をお勧めしています。 アップグレードの手順については、次を参照してください。[ハウツー： 仮想インターネット ルーティング ラボ インスタンスを Cisco Modeling Labs - Personal v2.0 へのアップグレード]

Cisco VIRL-PE リリース 2.0 に移行できないスタンドアロン展開のお客様には、UWM インターフェイスを介してリリース 1.6.66 にアップグレードして、salt-master サービスを無効にすることをお勧めします。 アップグレードの手順は、 http://get.virl.info/upgrd.1.3.php をご覧ください。

リリース1.5 またはリリース1.6 を実行し、クラスタモードを展開しているお客様には、salt-master サービスが無効にされて修正済みの SaltStack バージョンにアップグレードされるように、UWM インターフェイスを通してリリース 1.6.67 にアップグレードすることを推奨します。 リリース1.3 を実行しているお客様は、最新のリリース 1.6 に移行することを推奨します。

シスコでは、VIRL-PE リリース 1.6.67 でこの脆弱性を修正しました。 このリリースでは、両方の脆弱性の修正を含む SaltStack のバージョンにアップグレードされます。 ソルトサービスが無効な 1.6.66 を実行しているお客様も、リリース1.6.67 にアップグレードすることが推奨されます。

Cisco TelePresence IX5000 シリーズ

製品がサポート終了となったため、シスコは Cisco TelePresence IX5000 シリーズの修正版のソフトウェアをリリースしません。 Cisco TelePresence IX5000 シリーズでソルトサービスを完全に無効にするには、起動スクリプトファイルに変更を加える必要があります。これにはデバイスへの*ルートアクセス*が必要です。 サポートについては、サポート組織を通して Cisco TAC にお問い合わせください。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）は、これらの脆弱性のさらなるエクスプロイトが試みられたことを認識しました。 これらの脆弱性が修正済みソフトウェアリリースにアップグレードすることを、引き続き強くお勧めします。

出典

これらの脆弱性は、2020 年 4 月 29 日にソルトオープンコアチームによって公開されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-salt-2vx545AG

改訂履歴

バージョン	説明	セクション	ステータス	Date
2.0	脆弱性のある製品に Cisco TelePresence IX5000 シリーズを追加しました。 Cisco VIRL-PE と Cisco CML の修正済みのリリースとして、リリース 1.6.67 を追加しました。	「概要」、「脆弱性のある製品」、「回避策」、「修正済みソフトウェア」	最終版	2020 年 6 月 17 日
1.0	初回公開リリース		最終版	2020 年 5 月 28 日

利用規約