Y324470201.doc

Joint Security and Privacy Committee

NEMA COCIR JIRA

International Medical Informatics

医用情報システム上の
市販ソフトウェアのパッチ

2004-10

事務局: NEMA (National Electrical Manufacturers Association) www.nema.org/medical
1300 North 17th Street, Suite 1847, Rosslyn, VA 22209 USA tel: 703-841-3200 fax: 703-841-5900
書記: Stephen Vastagh, tel: 703-841-3281; fax: 703-841-3381 E-mail ste_vastagh@nema.org

1. 目的と適用範囲

医用情報システム (MedIS[1])では、ＯＳ、ブラウザ、データベースなどの市販のソフトウェア（COTSソフトウェア)を使用することが多くある。COTSソフトウェアのベンダー（供給メーカー）は、セキュリティ、プライバシー、または安定性などの問題を修正するためにパッチを当てることがよくある。これは「ホットフィクス」または「アップデート（更新）」ともよばれている。通常、COTSソフトウェアベンダーの試験または更新手順では、MedISで義務づけられている安全性・有効性の要求事項までは対応していない。つまり、医療サービス提供者はMedISで使用されているCOTSソフトウェアにパッチを当てる場合は、通常とは別の手順を踏まなければならない。

本文書の目的は、MedIS ベンダーに義務づけられる特別な要求事項、および COTS ソフトウェアにパッチを当てる際に直面する実用面での制限について医療サービス提供者に認識してもらうことである。

COTS ソフトウェアではなく、医用アプリケーションソフトウェアそのものを更新する場合は本白書の適用外となる。そのような更新は、MedIS ベンダーが適合する品質システムで要求されるコンフィギュレーション管理手順に従って実施される。同様に、脆弱性を修正するのではなく単に機能を追加するような更新も本文書の適用外となる。

ネットワークのセキュリティはMedISベンダーとユーザの両者が責任を共有するものであり、協力して問題の解決にあたる必要がある。パッチは、適切な「縦深防御」戦略の一部にしかすぎない。悪意のこもったソフトウェア（マルウェア）に対する防御に関しては広範な検討がなされ、「悪意のこもったソフトウェアに対する医用情報システムの保護」と題されたSPC白書にて述べられている。[2]

2. はじめに

IT システム全般を脅かす驚異は世界中で増大しているが、その一因となっているのが、システムの脆弱性を利用した悪意のこもったソフトウェアであり、MedIS ベンダーおよび医療サービス提供者もその影響を受けている。そのような脆弱性において最も弱いところを悪用することで、悪意のあるユーザが MedIS を支配して使用不可にしたりデータを壊してしまう可能性がある。

マルウェアに対抗し新たに出現する IT の脆弱性に対応するためには、IT システムのソフトウェアコンポーネントを定期的に更新する必要があるだろう。オフィス環境では、医療サービス提供者が自身でそのような更新を頻繁に行っている。一方、MedIS 上のパッチの配布は、下記の項目を含む特別な要求事項を満たさなければならない。

[1] MedIS generally includes all information systems directly employed in delivering health care. Examples include, but are not limited to: HIS (Hospital Information System), PACS (Picture Archiving and Communication Systems), imaging modalities, radiation therapy systems, and patient monitoring systems.
[2] The full text is available at http://www.nema.org/medical/spc.

- MedIS ベンダーおよび医療サービス提供者は、法律または契約によって、製品の安全性および臨床機能の有効性が維持されていることを保証しなければならない。
- 適切な試験を行って、MedIS 上のパッチが、患者に対して予期せぬ副次的な悪影響（性能または機能）を与えないように検証する必要がある。

上記の要求事項を満たすために、MedIS に関わる更新は MedIS ベンダーが関与するべきである。MedIS ベンダー によって定義された必要な手順および医療サービス提供者が遵守する手順を下記に記載する。

3. パッチ配布:ニーズと制限

この章では、MedIS のパッチ配布プロセスにおける標準的なステップを示す。そして各ステップをどう実施するかに関して、関係者に要求され項目と現在直面する制限を示す。

3.1 リリース状況の把握

COTS ソフトウェアベンダーが新たに発見された脆弱箇所を解消するパッチをリリースすることによって、更新手順が開始される。ベンダーおよびユーザは、新たな脆弱性の出現を適時、把握する必要がある。ものによっては即座に対策を打たなければいけないためである。MedIS ベンダーは、自社製品が使用している COTS ソフトウェアのパッチのリリース状況を監視する。ユーザも、ユーザの IT インフラ全体に及ぶリスクを考えれば、パッチのリリース状況を監視するべきである。パッチのリリース件数および安全性に対する影響の低さを考慮すると、ベンダーがパッチ配布時にユーザに通知するのは実用的でない。

3.2 脆弱性のリスク評価

パッチが公開された場合はまず、そのパッチで修正した脆弱性がもつ潜在リスクを理解しなければならない。MedISベンダーは、脆弱性がシステムの適切および安全な運用に与える影響を評価しなければならない。評価の際には、脆弱性が悪用される可能性、および悪用された場合にMedISや他のシステムに与える影響の両者を検討しなければならない。脆弱性の重大度を評価するために、「一般的な脆弱性と暴露性（CVE)」[3]分類システムを共通の用語として使うことができる。実際の驚異は、各MedIS製品または製品カテゴリーによって異なり、COTSソフトウェアがどのように使用されているかに依存する。
様々な軽減要素によって、脆弱性がセキュリティに与える潜在的な影響を軽減、または排除することさえもできる。無効となっている、または MedIS にインストールされていないコンポーネントに影響する脆弱性、もしくはシステムに与えるリスクが最小限で

[3] http://cve.mitre.org

ある脆弱性の場合は、MedIS ベンダーがパッチをリリースしないと判断することが可能である。

3.3 パッチの影響分析

パッチそのものが MedIS に与えるかもしれない潜在的影響を把握する必要もある。通常、パッチのインストールは、複数の COTS コンポーネントの動作またはインタフェースに影響を与えるが、これらのコンポーネントが他の MedIS ソフトウェアと相互に作用する。これらの相互作用を確認し評価するのは複雑で、MedIS ベンダーにかなりにの時間と労力を要するものかもしれない。パッチのほうが脆弱性よりも悪影響を与えてしまうことすら考えられる。ベンダーは、アップデートが失敗した場合の影響も考慮する。

ベンダーがリリースすることに決定したパッチに対しパッチの影響分析をすることによって、バリデーション（妥当性確認）戦略の方向性、およびどの機能を試験すべきかが分かるようになる。

許容できないリスクのあるパッチに対しては、MedIS ベンダーはリスク低減対策を決めて実施する必要がある。残留リスクは許容可能な範囲に入っていなければならない。

3.4 パッチのバリデーション（妥当性確認）

MedIS ベンダーは、適切に保守管理された自社製品が適切に機能することを保証する必要がある。パッチがインストールされる前に MedIS ベンダーはパッチのバリデーションを実施しなければならないことを医療サービス提供者が理解しておくのは大切である。MedIS ベンダーは、自社が提供するパッチの承認に対し最終責任を持つ。

正式なバリデーションのプロセスは、関連する法規制に適合しなければならないが（例：MedIS が米国で販売されている医療機器の場合はＦＤＡ）、少なくとも下記の事項を保証することが要求される。

- パッチを当てた MedIS が、意図したとおり機能し続けること。
- パッチは、COTS ソフトウェアベンダーが提示した仕様を満たすこと。
- パッチは、MedIS の安全性および有効性を損なわないこと。
- パッチを当てた後も MedIS は法的要求に適合すること。
- パッチを当てた MedIS は保守できること。.
- パッチ自身にマルウェアが入っていないこと。

バリデーションプロセスに対し、MedIS ベンダーはかなりの時間と努力をさく必要があるかもしれない。

3.5 パッチの配布

バリデーションされたパッチを、パッチがインストールされる各システムに配布すること。パッチ配布プロセスそのものを定義しバリデーションする必要がある。これは MedIS ベンダーがバリデーションしてリリースしたパッチが、特定の MedIS に配布されること保証するためである。基本的要求事項として下記がある。

- パッチのインテグリティーを維持する形で配布しなければならないが、採用された配布媒体によって方法が異なる。例、物理的な媒体（CD-ROM またはフロッピーディスク）またはデータネットワーク上で該当ソフトウェアアップデートをファイルとして転送する。
- 配布担当者が、配布が成功したかどうかはっきりと分かるような表示が必要である。

ベンダーが直面する実用面での制限によって、パッチが配布される速度と頻度に影響を与える可能性がある。

3.6 パッチのインストール

バリデーションされて配布されたパッチを各 MedIS 上にインストールすること。インストールに関しては、下記の事項が最小限要求される。

- 医療関連事業およびベンダーは、インストールが臨床現場での MedIS の運用の妨げにならないようにすること。例えば、仮に自動更新が適用される場合は、MedIS が患者に対して使用されていないときに限って更新がかかるよう計画すること。
- インストールを実施する担当者が、インストールのプロセスが成功したかどうかをはっきりと分かるように表示すること。
- インストールが失敗した場合は、MedIS を安全でバリデーションされた稼動状態に戻すこと。
- インストール手順には、新しく更新されたデバイスがインストール後、期待通り稼働していることを確認する方法も含めるべきである。

MedIS ベンダーは、サービススタッフの利用可能性、システムパッチの影響の性質、およびインストール処理を行うために必要なアクションの複雑さに基づいて、インストールの最善の方法を評価する。これには、最善のインストール処理が実現されるように、スタッフの利用可能性、患者のスケジュールに対する最低限の影響、および装置の利用可能性を保証するための、医療サービス提供者の関与も含まれる。例えば、インストールには、現場でのオンサイト・サポートが必要かもしれない、遠隔サービスで実施可能かもしれない、もしくはユーザ側の職員の協力が必要かもしれない。MedIS ベンダーが最善のインストールを実施するために決定するパッチの適用方法としては、個別のスケジューリング、定期的な実施、システムの更新時に合わせた実施などがある。

4. おわりに

ユーザは、ユーザの MedIS に使用されている COTS ソフトウェアを修正するパッチ関する情報をニュースや他の公開情報から入手することが出来る。多目的コンピュータで即座なパッチ対応に慣れている人は、MedIS ベンダーが MedIS に対し同じくらい迅速

にパッチを提供しないことに対し不満に感じるかもしれない。しかし、MedIS ベンダーが医療上の安全性および有効性の問題にも責任をもっていることをユーザは理解しなければならない。COTS ソフトウェアのセキュリティ、プライバシー、安定性に関するパッチの中には、パッチの配布にかかる費用と労力に見合ほど、安全性および有効性に関して重要ではないものもある。MedIS ベンダーは、リスク評価を通して、パッチの妥当性を評価する。

我々の目標は、MedIS ベンダーは適宜、適切なパッチをリリースする必要性を認識していることをユーザに確信してもらうことである。ベンダーは、自社のシステムの安全な稼働を維持する義務があり、それを厳しく受け止めている。この義務を果たすために、パッチに関するプロセスは前述したように時間を必要とする。MedIS ベンダーは、適切かつ安全なパッチを適切なタイミングでリリースする必要があることを認識している。ユーザが、ネットワークと MedIS を保護することで、この処理が進行している間の患者の安全を保護するために不可欠な手順を実施することも、同じように重要である。ユーザは、現実に存在する脅威の状況、MedIS のパッチの利用可能性、縦深防御戦略、ビジネスの継続性に関する計画などに基づいて、リスク評価戦略を作成する必要がある。

リスク評価およびバリデーションステップの省略は、マルウェアの攻撃を受け即座な対応が必要とされることを考えれば一見適切に思われるかもしれない。しかしそれは、MedIS ベンダーおよび医療サービス提供者の共通のミッションである適切な医療の提供を危険にさらすことになる。