2013 年 11 月 29 日
独立行政法人情報処理推進機構（IPA）

ICS-CERT モニター（2013 年 7 月/8 月/9 月号）概要

本概要は、米国土安全保障省の運営する ICS-CERT（Industrial Control Systems Cyber Emergency Response Team）発行の“ICS-CERT Monitor July, August, September 2013”の概訳となります。内容の詳細につきましては、原文をご参照ください。（※特記が無い限り、本文中のリンク先は、全て英語となります）
URL：
https://ics-cert.us-cert.gov/sites/default/files/Monitors/NCCIC_ICS-CERT_Monitor%20July-Aug-Sept.pdf

1. インシデント対応活動

（1）重要な製造業におけるインシデント

ICS-CERT では、重要な製造業で発生したインシデント支援を行った。事業者からハードドライブおよび仮想マシンのイメージのコピーの提出を受け、ICS-CERT にて解析を行ったところ、複数の業務システムでマルウェアが確認された。業務システムの 1 つに脆弱性対策が未実施だったアプリケーションがあり、事業者はこのシステムが感染源で、ユーザがスピアフィッシングメールを開いたことにより感染したと見ている。

現地で、オンサイト対応チームが業務ネットワークから SCADA ネットワークへの攻撃の可能性の検証や、Cyber Security Evaluation Tool（CSET）を用いた評価を行い、事業者と改善策について話し合った。

（2）インターネットに接続された制御システム

ICS-CERT では、インターネットからアクセス可能な制御システムについて注意喚起を行っている。

ある事例では、パスワードなしで直接アクセスできる冷暖房空調管理システムが確認された。運用は第三者に委ねられており、所有者から連絡を受けた第三者によって即座に認証が追加された。本件では所有者の対応が非常に速く、是正に要した時間は約 7 時間であった。

ICS-CERT では、自組織の制御システムがインターネットに接続されている／いない、どちらの現状認識に関わらず改めて監査を実施し、管理者権限レベルのデフォルトユーザーアカウントおよびパスワードが存在しない（削除されている）ことを確認するよう奨励している。

詳しくは、ICS-ALERT-11-343-01A および ICS-ALERT-12-046-01A を参照。

（3）インシデント対応および啓発活動

ICS-CERT と連邦捜査局（FBI）は、エネルギーや製造といった重要インフラ分野におけるインシデントのオンサイト対応を行った。ICS-CERT ではこれらのインシデントについて、US-CERT Secure Portal の制御システムセンター（Control Systems Center）を通じて以下の情報を公開している。

- 攻撃方法
- 攻撃者によるツール、戦術、手順（tools, tactics and procedures（TTPs））
- インシデントへの対応を通して学んだ教訓
- 侵入検知および既存のサイバーセキュリティ対策改善のための推奨および軽減施策

このようなインシデント対応のほか、事業者向けに機密扱いの情報を含む説明会を行う「Action Campaign」を再開した。説明会はワシントン DC、ニューヨーク、シカゴなどで行われた他、ビデオカンファレンスでも提供され、取り巻く脅威のについて最新の状況を伝えている。

2. インシデントの報告に関する FAQ

- インシデントとは？

一般的な定義としては、「明示されている、又は暗黙のセキュリティポリシーに違反する行為」であり、セキュリティポリシー（大まかには共通するものの、組織によって異なる）の存在が前提となる。米連邦政府機関では、NIST SP 800-61 の定義により、「セキュリティポリシーやコンピュータの利用規定、標準的なセキュリティ活動に対する違反行為又は差し迫った脅威」の発生を示す。（例：スピアフィッシングメール、サービス運用妨害（DoS）攻撃、不正アクセス、マルウェア、機器やソフトウェアの特性の不正な変更など）

参考：Federal Incident Reporting Guidelines（US-CERT）

- ICS-CERT に報告するのはどういう時か？

「インシデント」に該当するものは全て報告することを奨励しているが、とりわけ「標的型」な特性を持つインシデント（targeted in nature）については報告することが望ましい。（例：巧妙に細工されたスピアフィッシングメール、通常と異なる又は破壊的なマルウェア、制御環境における異常など）

また、制御システムに対する DoS 攻撃やスキャニンは、相関分析のため報告が望まれるほか、検知した事象が問題かどうか判断がつかない場合は、報告することを推奨している。

参考：Incident Handling Brochure（ICS-CERT）

3. トピックス

（1）制御システム環境におけるアプリケーションホワイトリスト（前編）

アプリケーションホワイトリスト（AWL）は、予め認可されたアプリケーションのみ実行を許可し、それ以外のアプリケーションは実行をブロックするセキュリティ技術である。実装にはファイルハッシュ、証明書、高信頼パス等の仕組みを利用する。AWL を導入する場合、それぞれの実装メカニズムの長所と短所を理解し、検討することが重要となる。また、多層防御の 1 レイヤとして利用することが望ましい。

- AWL が効果を発揮する攻撃、しない攻撃

一般に、AWL はインターネットからのダウンロードやファイル共有、外部ストレージメディア等を介して取り込まれた実行可能ファイルを用いた攻撃には効果があるが、サービス、ブラウザ、ワードや PDF などのフトウェアの脆弱性を悪用した攻撃を防ぐには効果が薄い。

- AWL の利点

仮にソフトウェアの脆弱性を悪用した攻撃が成功したとしても、攻撃の次段階を担うマルウェアの実行を困難にするなど、攻撃の持続性を妨げる効果が見込まれる（新しいマルウェアからの防御という点では、ホワイトリスト方式はウィルス対策ソフトのブラックリスト方式より効果的）。また、ネットワーク上の実行可能ファイルの集中的な監視・管理を可能にする。

- AWL の限界

AWL は、SQL インジェクションやメモリ破損など、認可されたアプリケーションの脆弱性を悪用した攻撃は防ぐことができない（但し、メモリベースの攻撃については、多くの AWL ソリューションで対策が講じられている）。また、Java Runtime や.NET Framework 等のよりハイレベルな実行環境で実行されるプログラムは、環境が認可されていれば実行を防ぐことができない。

※後編は次号に掲載予定です。

（2）同報無線の利用に伴うサイバーリスク

同報無線（Multi Address System Radio）は、その安価さ、柔軟性、使い易さから、制御監視（SCADA）システムにおいて幅広く使われている。同報無線は、1 対 N 通信（片方向又は双方向）で、通常 900MHz 帯を利用してリモートターミナルユニット（RTU）との通信を行う。同報無線には（とりわけ無線通信回線として使われている場合）多くの脆弱性があり、偽装、DoS 攻撃、中間者攻撃などが行われる可能性がある。2009 年の DEFCON では、軽自動車に収まるサイズの小型アンテナを使って DoS 攻撃を行い、通信妨害に成功した事例が報告されている。

Bradley Reeves 氏と Thomas Morris 氏は、2012 年に「産業制御システムに使用される狭域無線通信の脆弱性の分析と軽減策」と題した論文を発表し、以下の対策案を提示している。

- 帯域幅の使用を管理する
- 可能な限り指向性アンテナを使用する
- 無線機器を可能な限り地面近くに設置し、攻撃対象領域（attack surface）を限定する
- 『狭域』であることをセキュリティの拠り所にせず、他にもセキュリティ対策を講じる
- 定期的なリスクアセスメントを行う

4. 最近公開された脆弱性

※原文の RECENT PRODUCT RELEASES をご参照ください。

5. オープンソースニュース（ハイライト）

- セキュリティ研究者、「電灯もハッキングの標的になり得る」と警鐘（2013/08/14）
- ニューヨークタイムズ紙のウェブサイトがシャットダウン（2013/8/14）
- LIXIL 社のスマートトイレ「Satis」、スマホやタブレットからハッキング可能（2013/8/5）
- DEFCON で発表された最も恐ろしい 5 つのハッキング事例（2013/8/5）
- ハッカーら、「プリウス＆エスケープ」ハッキングの青写真を発表予定（2013/7/30）
- パイプラインからペースメーカーへ：エネルギー業界に倣い医療機器も安全性確保へ（2013/7/29）
- Google Glass の脆弱性を悪用し、QR コードの読み取りを通じてハッキング（2013/7/17）
- ハッカーらが見つけたコンピュータの脆弱性を、国家が買い取り（2013/7/13）
- 上下水道システムをサイバー攻撃から守る（2013/7/10）
- ICS-CERT：インターネットに接続された制御システム機器へのサイバー攻撃、「（結果的には）成功せず」（2013/7/8）
- 緊急警報システムに、リモートから偽の警報を流すことが可能な脆弱性（2013/7/8）
- オペラのコードサイニング証明書が盗まれ、マルウェアの配布に悪用される（2013/5/26）
- ドイツの学生、ラジコン飛行機に爆発物を仕掛け、テロを企む（2013/6/26）

6. 今後のイベント

※原文の UPCOMING EVENTS をご参照ください。

7. 協調的な脆弱性の公開（CVD）に協力頂いたセキュリティ研究者の方々

※ICS-CERT では、脆弱性を ICS-CERT に報告し、ベンダとの調整に協力くださったセキュリティ研究者の方々に感謝の意を表し、当該研究者の方々の功績として、氏名と対象の脆弱性の一覧を掲載しています。実際の氏名・脆弱性については、原文の COORDINATED VULNERABILITY DISCLOSURE を参照ください。

8. 脆弱性対策に協力頂いたセキュリティ研究者の方々（2013 年）

RESEARCHERS CURRENTLY WORKING WITH ICS-CERT IN 2013

ICS-CERT appreciates the following researchers who continue to work with us to resolve exploits:

Aaron Patterson	Dillion Beresford	Nadia Heninger
Aaron Portnoy	Eric Wustrow	Neil Smith
Alexey Osipov	Gleb Gritsai	Nin3
Andrew Brooks	Hisashi Kojima	Postive Technologies Security
Anton Popov	Ilya Karpov	Reid Wightman
Artem Chaykin	J. Alex Halderman	Roman Ilin
Arthur Gervais	Joel Langill	Rubén Santamarta
Billy Rios	John Adam Crain	Ryan Green
Bob Radvanovsky	Jon Christmas	Sergey Bobrov
Brendan Harris	Juan Vasquez	Sergey Gordeychick
Carlos Mario Penagos Hollmann	Jürgen Bilberger	Shawn Merdinger
Carsten Eiram	Kuang-Chun Hung (ICST)	Terry McCorkle
Cesar Cerrudo	Lucas Apa	Timur Yunusov
Christopher Scheuring	Luigi Auriemma	Zakir Durumeric
Christopher Sistrunk	Mashahiro Nakada	
Dale Peterson	Michael Toecker	

以上