2013 年 4 月 19 日
独立行政法人情報処理推進機構（IPA）

ICS-CERT モニター（2013 年 1 月/2 月/3 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 January/February/March 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、全て英文となります）

URL：http://ics-cert.us-cert.gov/pdf/ICS-CERT_Monitor_Jan-Mar2013.pdf

1. インシデントレスポンス活動

（1）スピアフィッシング攻撃、インターネット上でアクセス可能な公開情報を活用

2012 年 10 月に行われた米エネルギー業界を標的としたスピアフィッシング攻撃では、その前に開催された業界ミーティングのウェブサイトに掲載されていた出席者の氏名、所属会社名、役職、メールアドレスなどが、標的とするユーザの絞り込みや、メールの信憑性を高めるのに利用された。

ソーシャルメディアサイトや、職能団体、業界カンファレンスのウェブサイトなどに掲載されている一般公開情報は、攻撃者が詐欺メールの信憑性を高め、標的ユーザがメール内のリンクをクリックしたり、添付ファイルを開く確率を高める有益な情報として悪用されている。

スピアフィッシング攻撃の被害者になる確率を下げるため、組織体制やプロジェクト名といった業務関連情報や、役職や会社のメールアドレスといった個人情報をソーシャルメディアサイトに載せない、広告メールや不審なメール内のリンクをクリックしたり、添付ファイルを開いたりしないようすることが望ましい。スピアフィッシングやソーシャルエンジニアリングを避ける方法の詳細については Security Tip ST04-014 を参照のこと。

（2）認証／資格情報ストレージの脆弱性を利用したセキュリティ侵害

2012 年、ニュージャージー州のある製造会社の Tridium 社製 Niagara AX Framework を使った建物のエネルギー管理システムが、サイバー攻撃によって侵入された。攻撃者は SHODAN（インターネットに接続されているコンピュータ機器を検索できるサーチエンジン）を使って同社のシステムを見つけ、認証／資格情報ストレージの脆弱性を利用して侵入した。また、ある州政府の施設では、攻撃者が同様の手口を用いてやはりインターネットからアクセス可能な状態だったエネルギー管理システムに侵入し、温度設定を変更する事件が発生した。システムの脆弱性はセキュリティパッチにより是正されたが、これらの事件は、インターネットに接続されているシステムのセキュリティ対策の重要性を改めて浮き彫りにした。ICS-CERT と Tridium 社は、以下の対策を推奨している。

- 制御システムを直接インターネットに接続しない
- 認証／資格情報が記載されたファイル（config.bog）へのアクセス権を管理者レベルにしか付与しない
- ロックアウト機能を利用する
- 強度の高いパスワードを使用する
- デフォルトの認証情報を変更する
- Niagara AX Framework のマニュアルに従い、ファイルシステムへのユーザアクセスを制限する

（3）水飲み場型攻撃

水飲み場型攻撃は、最終的な標的である組織の従業員や関係者が関心を寄せている（訪れる可能性の高い）ウェブサイトにマルウェアを仕込み、標的組織のエンドユーザの PC に感染させることを狙う。最近の事例では、米外交問題評議会（CFR）と Capstone Tribune 社のウェブサイトに水飲み場型攻撃によってマルウェアを仕込まれ、複数セクタに跨る多くの重要インフラ事業者の PC が同ウェブサイトの閲覧によりマルウェアに感染していた。ICS-CERT では注意喚起を発して警告すると共に、感染の兆候に関する情報等を提供し、感染のチェックと対策の実施を促した。

2. トピックス

（1）国土安全保障省（DHS）、サイバーセキュリティ評価ツール（CSET）バージョン 5.0 をリリース

CSET は、制御システムおよびネットワークのセキュリティ対策の評価を通じてリスクとギャップを特定し、重要インフラにおけるセキュリティ対策の改善を支援している。CSET では、既存の業界基準を含め、全米で広く認められているサイバーセキュリティ基準に沿った評価を行うことができる。過去 1 年間に、DHS では全米各地で 80 以上の事業者の評価支援を行った。CSET は ICS-CERT のウェブサイトから無料でダウンロード可能。オンサイト支援の依頼や詳細については cset@hq.dhs.gov まで。

（2）過去 3 年間のセキュリティ評価結果に見る最も多い脆弱性

CSET を使ったセキュリティ評価も 3 年が経過し、ICS-CERT では 230 以上の事業者の評価支援を行った。これらの評価結果から、最も一般的なセキュリティギャップと脆弱性を整理した。

表：最も一般的な脆弱性

セキュリティ対策のカテゴリ	最も一般的な脆弱性
認可・権限・アクセス制御	・アクセス制御の不備
不適切な認証	・認証制御の不備
証明書・パスワード管理	・不十分な認証情報の保護 ・強度の低いパスワード
セキュリティ設定とメンテナンス	・テスト環境不備 ・パッチ管理不備、パッチ管理能力不備 ・バックアップおよびリストア能力不備
計画・ポリシー・手順	・ドキュメント化およびメンテナンス不備 ・正式なドキュメントの欠如 ・不十分な災害復旧計画
ネットワーク設計上の問題	・一般的な ICS ネットワーク設計上の弱点 ・セキュリティ境界の定義がない ・ネットワークのセグメント化がされていない ・実用的な DMZ が存在しない ・ファイアウォールが存在しない、または不適切に設定されている
ネットワーク構成機器の設定（実装の脆弱性）	・ネットワーク機器が適切に設定されていない ・ネットワーク機器にポートセキュリティが設定されていない ・侵入検知システム（ICS）の監視をしていない、または監視が足りていない

監査・説明義務	・セキュリティ監査／評価の欠如 ・ログを取っていない、または乏しい ・ネットワークアーキテクチャが良く理解されていない ・リモートログインポリシーがきちんと実行されていない ・送信／受信データの制御が弱い

（3）ログイン認証情報の保護

ユーザのログイン情報の保護は極めて重要である。ログイン情報を搾取しようとする場合に良く使われるのは「総当たり攻撃」（可能性のある組み合わせ等を全て試して正しいパスワードの発見を試みる攻撃）と「pass-the-hash 攻撃」（認証情報のハッシュを窃取し、同じ認証情報を使い回しているシステムへの侵を試みる攻撃）である。以下に、これらの攻撃が突こうとする問題点を減らすための対策方法を紹介する。

- *適切な権限管理* ： 管理用アカウント（例：Enterprise Admins アカウント、Domain Admins アカウント、ヘルプデスク用アカウント等）について、職務に応じた必要な権限のみを割り当て、階層化された適切な権限管理を行う。管理対象には、当該アカウントが使えるホストはどれか、管理者がその PC にアクセスする方法等も含める。例外が発生する場合は、一時的な専用アカウントを作成し、作業が終わったら即削除するか、使用が ACL や IPSec 等で厳格に制限された特定のホストでのみ実施させる等が望ましい。また、デフォルトで Administrators にしばしば許可されており、pass-the-hash 攻撃で多用される SeDebugPrivilege については、本当に必要とするユーザのみに許可を制限するため、特別なデバッグ用アカウントを作成し、run as で実行させるようにする。
- *ネットワーク／システムの設計およびポリシー*： 全社のネットワークについて、インターネット、DMZ、イントラネットの原則に基づき、異なる信頼度レベルのネットワークの接続を区切る。共通のイメージを適用する場合は、パスワードも共通となってしまうので注意が必要となる。ローカルの特権アカウントを無効化、変更、または削除し、全てのホストのローカルアカウントのパスワードが一意になるようにする。

3. ICS-CERT ニュース

DHS では体制の見直しを行い、CSET やオンサイト評価、ICSJWG フォーラム等、これまで Control System Security Program（CSSP）下で実施していた支援活動について、今後は ICS-CERT 下で提供することにした。

4. 最近公開された脆弱性

※原文の RECENT PRODUCT RELEASES を参照ください。

5. オープンソースニュース（ハイライト）

- ナポリターノ長官、DHS の将来的な目標、強制歳出削減措置について述べる（2013/2/26）
- DHS サイバーセキュリティ担当次官補佐、”Cyber 911“の設置、任意のサイバーセキュリティ基準の整備に意欲（2013/2/25）
- ハッキングされた Bit9 社、SQL インジェクションの脆弱性が原因であったと話す（2013/2/25）
- 米国へのハッキングに中国人民解放軍の部隊が関与か（2013/2/18）
- 中国人ハッカーの身元が判明（2013/2/14）
- 重要インフラのセキュリティおよびレジリエンスに関する大統領政策指令（2013/2/12）
- SCADA、ICS の脆弱性の売買市場、IT 脆弱性の売買市場に酷似（2013/2/5）
- Zeus のソースコードが闇市場で売りに出される（2013/2/4）

- オラクル社、Java のセキュリティアップデートを緊急発信（2013/2/4）
- 米オバマ大統領、軍事的サイバー攻撃に関して幅広い権限を保有（2013/2/3）
- 2,500 ドルでミッション・クリティカルな GPS ネットワークをシャットダウンする方法（2012/12/14）
- Skynet ― Tor を利用した防弾ボットネット（2012/12/10）
- "Dexter" ― POS 端末からクレジットカード情報を盗むマルウェア（2012/12/11）
- アラムコ社、サイバー攻撃は製油工程を狙ったものだったと話す（2012/12/9）
- 英政府職員、「我が国の重要インフラは既にサイバー攻撃に遭っている」と話す（2012/12/4）
- 重要インフラ業界のサイバーセキュリティ、他業界への見本となる可能性（2012/12/4）
- MySQL データベースをシャットダウンする脆弱性（2012/12/3）
- 2012：グローバルサイバー戦争の幕開け（2012/11/15）

6. 今後のイベント

6/17～21 開催予定の「Industrial Control Systems Cybersecurity (301) Training (5 days) North American Partners」（於：アイダホフォールズ）以外については中止。

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（2012 年）

RESEARCHERS CURRENTLY WORKING WITH ICS-CERT IN 2012

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

Aaron Patterson	Dale Peterson	Michael Toecker
Aaron Portnoy	Dillion Beresford	Neil Smith
Andrew Brooks	Nadia Heninger	Postive Technologies Security
Anton Popov	Eric Wustrow	Reid Wightman
Arthur Gervais	J. Alex Halderman	Rubén Santamarta
Billy Rios	Joel Langill	Sergey Gordeychick
Bob Radvanovsky	Jon Christmas	Shawn Merdinger
Brendan Harris	Juan Vasquez	Terry McCorkle
Carlos Mario Penagos Hollmann	Kuang-Chun Hung (ICST)	Zakir Durumeric
Carsten Eiram	Lucas Apa	
Cesar Cerrudo	Luigi Auriemma	

以上