2012 年 9 月 21 日
独立行政法人情報処理推進機構（IPA）

ICS-CERT マンスリー・モニター（2012 年 8 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 Monthly Monitor August 2012”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。（※本文中のリンク先は、全て英文となります）

URL：http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_August_2012.pdf

1. 8 月のインシデントレスポンス活動 － インターネットからアクセス可能な医療機器

医療機器についても、リモート監視が進んでいる傾向にある。制御システム同様、医療機器も正常な動作が損なわれることは致命的な結果を引き起こす可能性がある。医療施設においては、医療機器を直接インターネットに接続しないようにし、医療機器ベンダは、製品の提供前に埋め込み型医療機器のセキュリティ機能の実装や脆弱性の評価を行うべきである。もしベンダ自身にそのスキルがないのであれば、専門の会社に依頼することが奨励される。

最近の事例として、インターネットからアクセス可能な医療機器が大学で見つかった。実際に使用していたものか、研究の一環だったかは不明だが、システム管理者に連絡を取り、是正がなされた。

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対する脅威と対策を纏めたドキュメントも公開しているので参照のこと。

2. 今月のトピックス ― インドにおける大規模停電

7 月末から 8 月初めにインド北東部で発生した大規模停電の原因はサイバー攻撃ではなく、丁度干ばつの影響で農家が河川から水を引くのに通常以上の電力を使用していたタイミングで電力網の一系統が定期点検のために停止したことなどにより、電力の供給が需要に追い付けず電力網がパンクした為であり、結果的にインドの人口の半数近くが電力を失う事態となった。また、空港、鉄道、道路の信号、病院、上下水道システムなど、重要インフラも影響を受けた。元々インドでは公共電力網の信頼性が低く、無停電電源装置（UPS）や、ディーゼル発電機を備えている産業も少なくない。そうした備えが停電の影響を抑えたには違いないが、古いインフラ、経済の発展に伴い年々肥大する需要、更には、違法に電力網から電力を盗んでいる企業や住宅が問題を複雑にしている（デリーだけで、供給量の 42%が盗まれている）。こうした停電は今後も起きると予想され、インドでは電力システムの可視化やインフラの近代化が必須となっている。

原因はサイバー攻撃ではなかったが、悪意ある行為は影響を更に拡大させる。米国の重要インフラ事業者は、ICS-CERT のホームページに最新の脆弱性情報等が掲載されているので参照のこと。

3. Control System Security Program（CSSP）ニュース

（1）制御システムベンダの脆弱性公開ポリシーが公開される

Industrial Control Systems Joint Working Group（ICSJWG）のベンダ・サブグループ（Vendor subgroup）は、ICS ベンダと SIer が纏めたベンダ共通の脆弱性公開ポリシー“Common Vulnerability Disclosure Framework”を公開した。

（2）ICS-CERT、脆弱性公開ポリシーを更新

ICS-CERT は、脆弱性公開ポリシーを更新した。情報公開ポリシーの目的は、制御システム側とベンダ側の今回のシステムベンダ側のバランスを取って、調整することである。今回の更新では、ベンダの対応が鈍い場合、ベンダのパッチ準備や緩和策に関わらず、ベンダへの通知から 45 日目以降に脆弱性を公開することを追記している。

（3）DEF　CON 終了

7 月 26 日～29 日に米国ネバダ州ラスベガスで開催されたハッカーの祭典“DEF CON”終了。制御システムの脆弱性も幾つか報告され、ICS-CERT からも、2 件の注意喚起と 1 件のアドバイザリが出されている。

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. 今月のオープンソースニュース（ハイライト）

- DEF CON：交通システムのハッキング方法（2012/7/31）
- インド、史上最大規模の停電再び。6 億 8 千万人に影響（2012/7/31）
- 化学施設のテロ対策基準（CFATS）プログラムの導入に関する評価（2012/7/31）
- Black Hat のアンケート調査、36％が報復手段としてハッキングを行ったことがあると回答（2012/7/26）
- 米国が新しく導入する航空交通管制システムに脆弱性。Black Hat で研究者が指摘（2012/7/26）
- 研究者、IP アドレスをスキャンし、脆弱性を探すツールを公開。1 時間に 100 万の IP アドレスのスキャンが可能（2012/7/25）
- 研究者、スマートメータのハッキングツールを公開（2012/7/20）
- 北極で事業を展開している石油会社 5 社のシステムにハッカーが侵入、データが窃取される（2012/7/16）
- 研究者、世界 52 ヶ国の重要インフラで使われているシステムの脆弱性を公開（2012/7/13）
- 驚異の統合性を実現するビル設備の一括監視制御システム Niagara Framework に脆弱性（2012/7/12）
- オランダの大手化学会社 DSM、USB メモリ感染型ウィルスを用いたサイバー攻撃を撃退（2012/7/11）
- 嵐による停電、社会インフラの脆弱性を浮き彫りに（2012/7/2）
- 新国土安全保障省サイバーセキュリティ担当副次官 Mark Weatherford 氏、米国のサイバーセキュリティ対策にスーパーチームで臨む（2012/7/2）
- ICS-CERT が 2009 年～2011 年の活動レポートを公開。重要インフラのサイバーインシデントが急増（2012/6/29）

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（CVM）に協力頂いたセキュリティ研究者の方々（2012 年 8 月）

※原文の NOTABLE COORDINATED DISCLOSURE RESEARCHERS IN AUGUST 2012 をご参照ください。

以上