Japan Computer Emergency Response Team
Coordination Center

電子署名者 : Japan Computer Emergency Response Team Coordination Center
DN : c=JP, st=Tokyo, l=Chiyoda-ku, email=office@jpcert.or.jp, o=Japan Computer Emergency Response Team Coordination Center, cn=Japan Computer Emergency Response Team Coordination Center
日付 : 2012.03.02 10:43:04 +09'00'

JPCERT CC®

JPCERT/CC の取組みとツールの紹介

一般社団法人 JPCERT コーディネーションセンター
情報流通対策グループ　山田　秀和

本日のアジェンダ

I. JPCERT/CCのこれまでの取組み
II. JPCERT/CCのこれからの取組み
III. 制御システム向けツールの紹介
IV. S4
V. まとめ

Copyright® 2012 JPCERT/CC All rights reserved.

I. JPCERT/CCのこれまでの取組み

II. JPCERT/CCのこれからの取組み

III. 制御システム向けツールの紹介

IV. S4

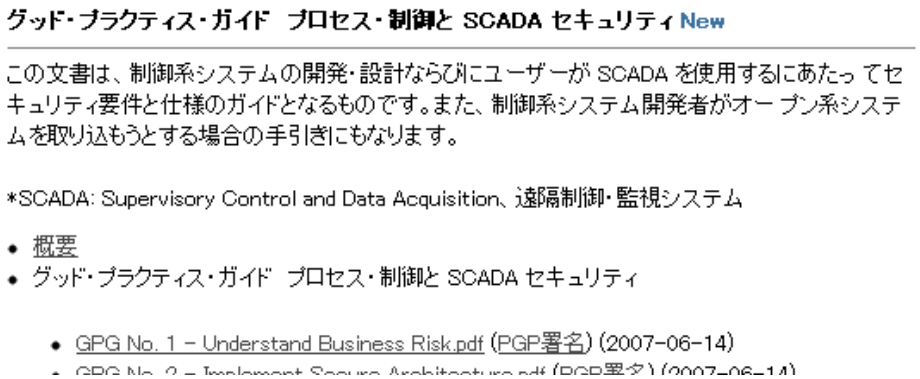
V. まとめ

Copyright® 2012 JPCERT/CC All rights reserved.

JPCERT/CCのこれまでの取組み

2007年の取組み

グッド・プラクティス・ガイド プロセス・制御とSCADAセキュリティ



グッド・プラクティス・ガイド　プロセス・制御と SCADA セキュリティ New

この文書は、制御系システムの開発・設計ならびにユーザーが SCADA を使用するにあたって セキュリティ要件と仕様のガイドとなるものです。また、制御系システム開発者がオープン系システムを取り込もうとする場合の手引きにもなります。

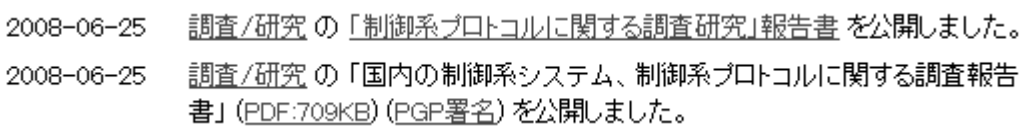
*SCADA: Supervisory Control and Data Acquisition、遠隔制御・監視システム

- 概要
- グッド・プラクティス・ガイド　プロセス・制御と SCADA セキュリティ
  - GPG No. 1 – Understand Business Risk.pdf (PGP署名) (2007-06-14)
  - GPG No. 2 – Implement Secure Architecture.pdf (PGP署名) (2007-06-14)

2008年の取組み

「制御系プロトコルに関する調査研究」報告書

国内の制御システム、制御系プロトコルに関する調査報告書



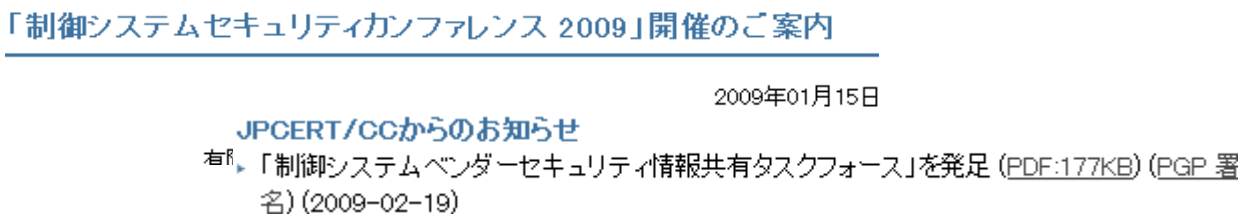
2008-06-25　調査/研究 の「制御系プロトコルに関する調査研究」報告書 を公開しました。

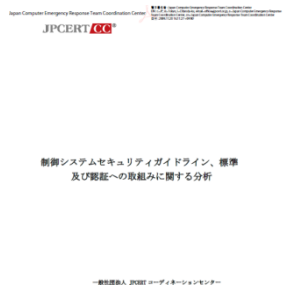
2008-06-25　調査/研究 の「国内の制御系システム、制御系プロトコルに関する調査報告書」(PDF:709KB) (PGP署名) を公開しました。

Copyright® 2012 JPCERT/CC All rights reserved.

JPCERT/CCのこれまでの取組み

- 2009年の取組み
  - 制御システムセキュリティガイドライン、標準、及び認証への取り組みに関する分析
  - 重要社会インフラのためのプロセス制御システム（PCS）のセキュリティ強化ガイド
  - 制御システムベンダーセキュリティ情報共有タスクフォース
  - 制御システムセキュリティカンファレンス 2009
  - 制御システムセキュリティ関連情報（メーリングリスト）





Copyright® 2012 JPCERT/CC All rights reserved.

JPCERT/CCのこれまでの取組み

- 2010年の取組み
  - 推奨プラクティス：工業用制御システムにおけるサイバーセキュリティインシデント対応能力の開発
  - 人的セキュリティガイドライン
  - 制御システムのサイバーセキュリティ：多層防御戦略
  - 制御システム環境におけるサイバーセキュリティ文化の支援を目的とした運用セキュリティ（OPSEC）の使用
  - グッド・プラクティス・ガイド パッチ管理
  - グッド・プラクティス・ガイド プロセス・制御とSCADAセキュリティ(改訂)

制御システムセキュリティカンファレンス2010

制御システムセキュリティ情報共有タスクフォース

- 制御システムベンダに限らず、制御システムに携わる方を対象

Copyright® 2012 JPCERT/CC All rights reserved.

JPCERT/CCのこれまでの取組み

2011年の取組み


制御システムセキュリティカンファレンス2011


制御システムセキュリティアセスメントツール(SSAT)の提供開始


制御システムセキュリティ検討タスクフォース
インシデントレスポンス体制検討ワーキンググループ事務局

Copyright® 2012 JPCERT/CC All rights reserved.

I. JPCERT/CCのこれまでの取組み
II. JPCERT/CCのこれからの取組み
III. 制御システム向けツールの紹介
IV. S4
V. まとめ

Copyright® 2012 JPCERT/CC All rights reserved.

2012年の取組み（予定）


インシデント対応に必要な技術および実態の調査

ポータルサイト


制御システムセキュリティアセスメントツール


セキュアコーディング


脆弱性情報ハンドリング

Copyright® 2012 JPCERT/CC All rights reserved.

インシデント対応に必要な技術および実態の調査

日　時	3月中旬実施予定
期　間	2日間
内　容	Idaho の実地訓練から得た経験をもとに制御シミュレータ等を用いた擬似制御環境を用いて組織でのインシデント対応を行う上で必要と考えられる項目の調査等を実施
対　象	ユーザ + ベンダの2人1組
募集数	最大で10組(20人程度)

Copyright® 2012 JPCERT/CC All rights reserved.

ポータルサイト

- ポータルサイトでの情報提供
  - 現在のメーリングリストでの配信も残しつつポータルサイトでの情報提供も検討中
    - メーリングリストでの配信内容見直しも
  - 特定期間内に収集した制御システムセキュリティ関連の情報
  - 記事へのアクセス数や反響の大きい情報を中心に分析や追跡調査などを行う予定
- 対象者
  - 制御システムベンダー
  - 制御システムユーザー
- 利用に当たって（現在検討中）
  - NDA
  - 組織としてのセキュリティ対応チームの確立

Copyright® 2012 JPCERT/CC All rights reserved.

制御システムセキュリティアセスメントツール

JPCERT CC®

- 制御システムセキュリティアセスメントツール（日本版SSAT）
  - 各管理項目における現状を「見える化」する
  - 問題発見や気づくためのきっかけ作り
  - 設問数の100問前後
  - 1/31 時点での JPCERT/CC からの直接配布数 89
  - 本ツールはベンダやユーザ、業界団体がカスタマイズを加えるなどして再配布することも可能

Copyright® 2012 JPCERT/CC All rights reserved.

制御システムセキュリティアセスメントツール

2011年のアセスメントツール提供時

全面的にご協力をいただいたセキュリティ合同WGの皆様

- SICE（公益社団法人計測自動制御学会）
  計測・制御ネットワーク部会セキュリティある情報共有検討WG
- JEITA（社団法人電子情報技術産業協会）
  制御・エネルギー管理専門委員会　安全・安心システムWG
- JEMIMA（社団法人日本電気計測器工業会）
  PA・FA計測制御委員会セキュリティ調査研究WG

また、昨年末より以下の皆様にもご協力いただき

- **業界団体、各企業ご担当者様**

日本の制御システム業界に適した形でのアップデート作業進行中

Copyright® 2012 JPCERT/CC All rights reserved.

JPCERT CC®

セキュアコーディング （C/C++ / Java）

- 出荷後のソフトウエア製品に発見される多くの脆弱性は、プログラミングエラーによって引き起こされている。
- 製品開発工程において、脆弱性につながるような欠陥を作りこまない、仮に作りこまれたとしても出荷前の検証等の段階で発見・対応につながる取り組みが必要。
- 開発工程別、あるいは、開発プロセスを包含したよりセキュアな製品開発を実施するための幾つかの対策アプローチが存在する。

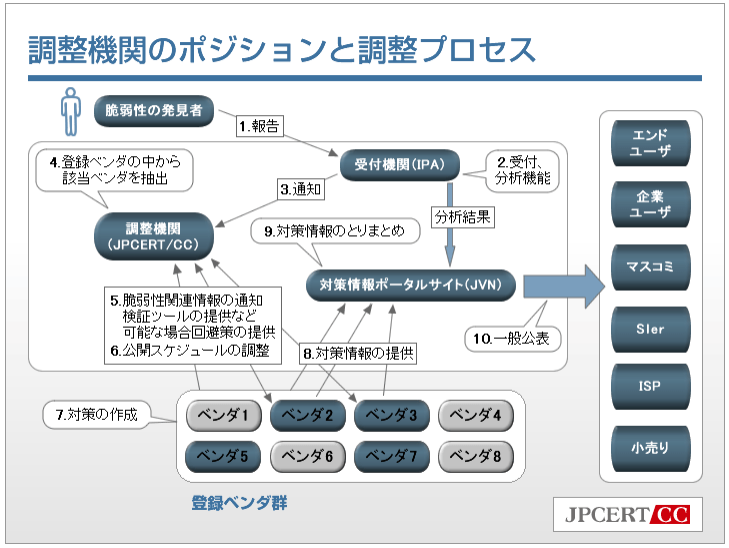
セキュアコーディング

Copyright® 2012 JPCERT/CC All rights reserved.

脆弱性ハンドリング

脆弱性ハンドリング

一般公表前のソフトウエア/ハードウエアシステム等におけるセキュリティ上の欠陥に係わる情報を、適切な方法で取り扱い、製品開発者によって用意された対策情報とともに公表することによって問題解決方法を広く示し、社会における製品利用者の安全に貢献するための活動



Copyright® 2012 JPCERT/CC All rights reserved.

脆弱性ハンドリング

JPCERT CC®

- 制御システム関連情報の公表例①
  - JVN#98649286 (2011/11/01) https://jvn.jp/jp/JVN98649286/
    CSWorks の LiveData Service におけるサービス運用妨害 (DoS) の脆弱性

公開日:2011/11/01 最終更新日:2011/11/02

JVN#98649286
CSWorks の LiveData Service におけるサービス運用妨害 (DoS) の脆弱性

概要
CSWorks のサーバコンポーネントの一部である LiveData Service には、サービス運用妨害 (DoS) の脆弱性が存在します。

影響を受けるシステム

- CSWorks 2.0.4115.0 およびそれ以前

詳細情報
CSWorks のサーバコンポーネントの一部である LiveData Service には、TCP パケットの処理に起因するサービス運用妨害 (DoS) の脆弱性が存在します。

想定される影響
遠隔の第三者により、サービス運用妨害 (DoS) 攻撃を受ける可能性があります。

対策方法
アップデートする
開発者が提供する情報をもとに最新版へアップデートしてください。

ベンダ情報

ベンダ	リンク
CSWorks	Important: CSWorks 2.0.4115.1 security release
	Release History

Copyright® 2012 JPCERT/CC All rights reserved.

脆弱性ハンドリング

JPCERT CC®

CSworks 社の情報公開

CSWorks: web-based industrial automation

Of CSWorks and software development

<< PostgreSQL support | CSWorks 2.1.4386.0 released >>

Important: CSWorks security release 2.0.4115.1

10月 27, 2011 09:23 by Sergey Sorokin

Date: October 27, 2011
Subject: DoS vulnerability in CSWorks LiveData Service
Versions: 2.0.4115.0 and earlier
Summary: Remote attackers can perform a denial of service(software crash).

Description
CSWorks LiveData Service 2.0.4115.0 and earlier allows remote attackers to cause a denial of service after sending crafted TCP packets. Isolating communication between CSWorks LiveData Service and web servers that accept requests from client applications mitigates the issue.

Patch availability
CSWorks 2.0.4115.1 has been issued as security release to correct the defect. CSWorks administrators running affected versions are advised to upgrade to 2.0.4115.1 as soon as possible. The security release can be downloaded from CSWorks web site http://www.controlsystemworks.com/DownloadDescription.aspx.

Credits
The vulnerability was reported by Kuang-Chun Hung, Security Research and Service Institute - Information and Communication Security Technology Center (ICST), Taiwan R.O.C

References
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3996 (will be available after confirmation by MITRE)
http://jvn.jp/en/jp/JVN98649286/index.html (will be available after confirmation by JPCERT/CC)

http://www.controlsystemworks.com/blogengine/post/CSWorks-2041151-security-release.aspx

Copyright® 2012 JPCERT/CC All rights reserved.

脆弱性ハンドリング

制御システム関連情報の公表例②

- JVN#63249231　https://jvn.jp/jp/JVN63249231/
  Cogent DataHub における HTTP ヘッダインジェクションの脆弱性
- JVN#12983784　https://jvn.jp/jp/JVN12983784/
  Cogent DataHub におけるクロスサイトスクリプティングの脆弱性

公開日:2012/01/11　最終更新日:2012/01/12

JVN#63249231
Cogent DataHub における HTTP ヘッダインジェクションの脆弱性

概要
Cogent Real-Time Systems Inc. の提供する Cogent DataHub には、HTTP ヘッダインジェクションの脆弱性が存在します。

影響を受けるシステム

- Cogent DataHub V7.1.2 およびそれ以前
- OPC DataHub V6.4.20 およびそれ以前
- Cascade DataHub V6.4.20 およびそれ以前

詳細情報
Cogent Real-Time Systems Inc. の提供する Cogent DataHub には、HTTP ヘッダインジェクションの脆弱性が存在します。

想定される影響
ユーザのウェブブラウザ上で偽の情報が表示されたり、HTTP レスポンス分割攻撃を受けたりするなどの可能性があります。

対策方法
アップデートする
開発者の提供する情報をもとに、最新版にアップデートしてください。

ベンダ情報

ベンダ	リンク
Cogent Real-Time Systems Inc.	Release Notes
	Download Software

公開日:2012/01/11　最終更新日:2012/01/12

JVN#12983784
Cogent DataHub におけるクロスサイトスクリプティングの脆弱性

概要
Cogent Real-Time Systems Inc. の提供する Cogent DataHub には、クロスサイトスクリプティングの脆弱性が存在します。

影響を受けるシステム

- Cogent DataHub V7.1.2 およびそれ以前
- OPC DataHub V6.4.20 およびそれ以前
- Cascade DataHub V6.4.20 およびそれ以前

詳細情報
Cogent Real-Time Systems Inc. の提供する Cogent DataHub には、クロスサイトスクリプティングの脆弱性が存在します。

想定される影響
ユーザのウェブブラウザ上で任意のスクリプトを実行される可能性があります。

対策方法
アップデートする
開発者の提供する情報をもとに、最新版にアップデートしてください。

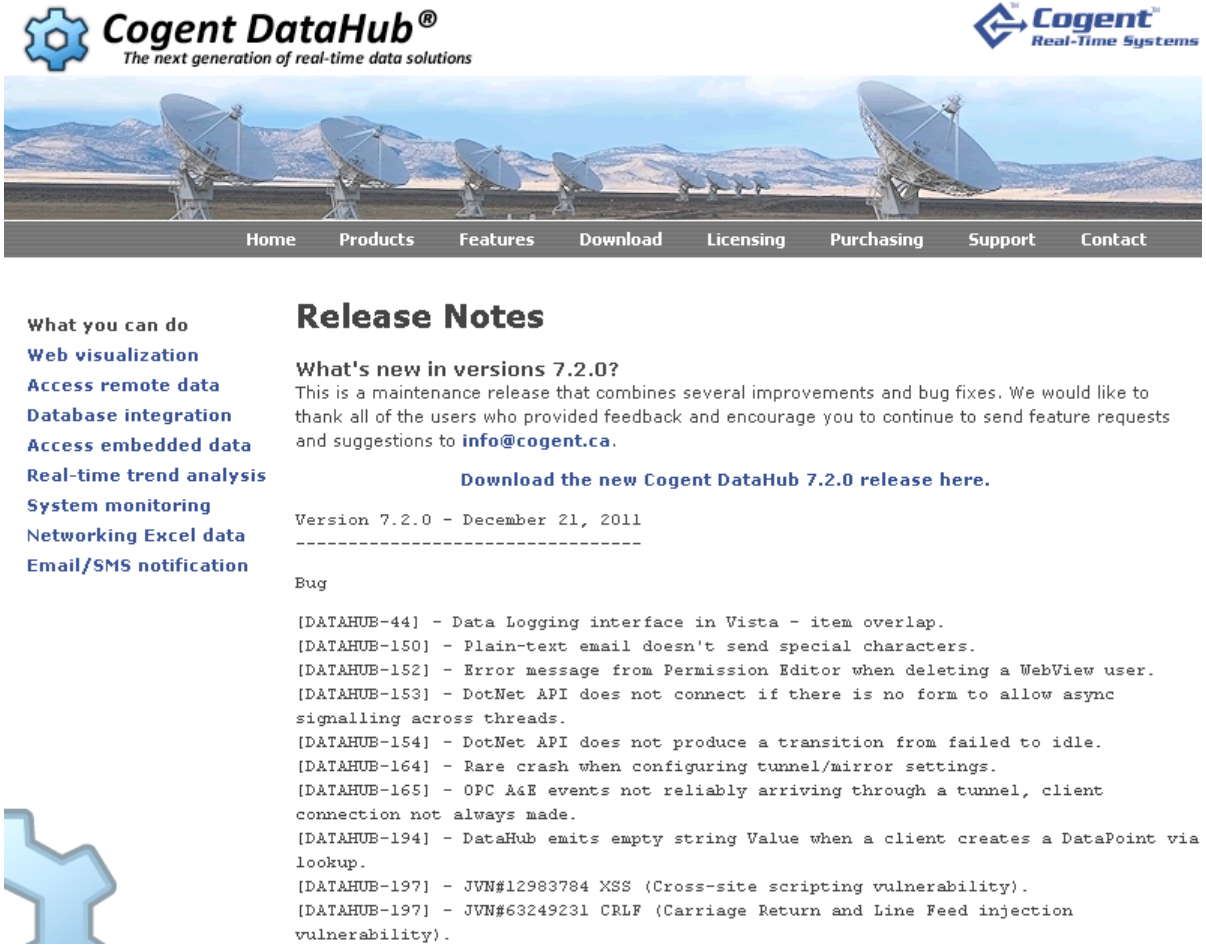
ベンダ情報

ベンダ	リンク
Cogent Real-Time Systems Inc.	Release Notes
	Download Software

Copyright® 2012 JPCERT/CC All rights reserved.

脆弱性ハンドリング

- Cogent 社の情報公開



http://www.cogentdatahub.com/ReleaseNotes.html

Copyright® 2012 JPCERT/CC All rights reserved.

I. JPCERT/CCのこれまでの取組み
II. JPCERT/CCのこれからの取組み
III. 制御システム向けツールの紹介
IV. S4
V. まとめ

Copyright® 2012 JPCERT/CC All rights reserved.

制御システム向けツールの紹介

- Bandolier
  - Digital Bond 社がDoEからの資金を元に作成
  - 制御システムに最適なセキュリティ設定を確認するための監査ファイル（カスタマイズ可能）
  - Nessus（脆弱性スキャナ）のプラグインとして提供

Copyright® 2012 JPCERT/CC All rights reserved.

制御システム向けツールの紹介

JPCERT CC®

- ツールの利用場面
  - ベンダーの皆様
    - 社内の品質保証
    - 受け入れテスト時

  - ユーザーの皆様
    - 受け入れテスト時
    - 定期的なセキュリティテスト

List of Bandolier Security Audit Files

Bandolier Security Audit Files help asset owners and vendors identify and audit optimal security configuration for control system servers and workstations. In this Department of Energy funded project, Digital Bond partners with leading control system application vendors to establish practical security configuration guidance for SCADA, DCS, and other industrial control system components. Digital Bond then creates and distributes specialized security audit files that can be used with the Nessus vulnerability scanner. Bandolier, in conjunction with Nessus, is the most widely used security tool in industrial control systems.

The Bandolier Baselines represent the OS vendor / industry advice for the best practice security configuration that is then slightly modified for settings that will cause problems for control systems. Below are the available Bandolier Baselines.

Vendor	OS Name
Microsoft	Windows 7
Microsoft	Windows Server 2008 R2

Below is the list of Bandolier Security Audit Files and their current status.

Vendor	Application Name	Version	Operating System	Status
ABB	800xA PPA Connectivity Server	5.x	Windows Server 2003	1.0
ABB	800xA PPA Aspect Server	5.x	Windows Server 2003	1.0
ABB	800xA PPA Historian	5.x	Windows Server 2003	1.0
ABB	800xA PPA Domain Controller	5.x	Windows Server 2003	Development
ABB	800xA PPA Engi/Operator Workplace	5.x	Windows XP	1.0
Alstom Grid	e-terraplatform (Production Server)	2.5	Windows Server 2003	1.1
Alstom Grid	e-terraplatform (Production Server)	2.5	Red Hat Linux 5.3	1.1
Alstom Grid	e-terraplatform	2.6	Windows Server	1.0

CSI Control Systems International	UCOS FCU App Server	1.0	CENTOS	1.0
CSI Control Systems International	UCOS Operator Work Station	5.2	Windows 7	1.0
CSI Control Systems International	UCOS PHA – Historian	5.2	Windows 2008 Server R2	1.0
Emerson	Ovation Engineering Workstation	3.1	Windows XP	1.0
Emerson	Ovation Operator Workstation	3.1	Windows XP	1.0
Emerson	Ovation Process Historian	3.1	Windows Server 2003	1.0
Emerson	Ovation SCADA Communication Server	3.1	Windows Server 2003	1.0
Matrikon	Security Gateway Tunneller		Windows Server 2003	1.1
OSIsoft	PI Enterprise Server	3.3.x 3.4.x	Windows Server 2003	1.3.7
Siemens	Spectrum Power TG SCADA Host	8.2	Red Hat Linux	1.1
Siemens	Spectrum Power TG SCADA Workstation	8.2	Windows XP	1.1
Siemens	Spectrum Power TG Web Console	8.2	Windows Server 2003	1.1
SISCO	AX-S4 ICCP Server	4.0059.2	Windows Server 2003	1.1
SNC-Lavalin ECS	GENe SCADA	GENe	Red Hat Linux	1.1
Talvent	OASyS DNA Realtime Server	7.5	Windows Server 2003	1.1

TENABLE PRODUCTS

Nessus

Nessus Product Overview

Tenable Nessus® vulnerability scanner is the world-leading vulnerability scanner. With more than five million downloads to-date, Nessus features high-speed discovery, configuration auditing, asset profiling, sensitive data discovery and vulnerability analysis of your security posture. Nessus scanners may be distributed throughout an entire enterprise, inside DMZs and across physically separate networks.

- Product Overview
  - Features
  - Nessus for Business
  - Nessus for Home
  - Upgrade to Nessus 4.4
  - Nessus Mobile Apps
- Nessus Auditor Bundles
- Nessus Plugins
- Documentation
- Nessus FAQ
- Sample Reports
- Deployment Options
- Training

Nessus 4.4 Screenshots

TENABLE PRODUCTS

PF

SCADA Checks

The Tenable Nessus ProfessionalFeed contains, in addition to the regular network vulnerability checks, several dozen plugins for Nessus 4 that specifically discover and test SCADA devices.

The SCADA family of plugins will readily produce vulnerability audit data that can be leveraged for a variety of NERC and other types of security audits involving process control networks. In the power industry, this can help create various lists of devices by active SCADA protocol (ICCP, DNP3, etc.) as well as function or even "Area of Responsibility".

For NERC compliance, this process can help make sure the list of "Critical Cyber-Security Assets" is accurate and does not include too many hosts while ignoring others.

In addition, through funding by the Department of Energy, Digital Bond has produced a wide variety of audit policies for Nessus users to test the configurations of many different types of Unix and Windows control system software.

Both Tenable and Digital Bond have written extensively about SCADA and Control Systems auditing in their blogs:

- Bandolier and NERC CIP
- Extending Bandolier with Other Nessus Credential Checks
- Bandolier Security Audit File Release: MatrikonOPC
- Nessus SCADA Plugins

If you are an enterprise customer, you should consider applying Tenable's Unified Security Monitoring approach to NERC and control systems monitoring. We've produced a short video entitled Auditing Scada and Control System Networks that shows how our passive, active and log analysis products can be used to monitor control system networks.

- Product Overview
- Nessus Product Overview
- Nessus Plugins
- Policy Compliance Checks
- SCADA Checks
- Deployment Options
- Commercial Support
- Purchase Now
- Evaluate Now

Copyright® 2012 JPCERT/CC All rights reserved.

I. JPCERT/CCのこれまでの取組み

II. JPCERT/CCのこれからの取組み

III. 制御システム向けツールの紹介

IV. S4

V. まとめ

Copyright® 2012 JPCERT/CC All rights reserved.

S4 (Scada Security Scientific Symposium)

JPCERT CC®

- S4(Scada Security Scientific Symposium)とは
  - 2007から米国で開催されている制御システムのセキュリティに特化したカンファレンス(2011年は開催せず)
  - 開催時期:毎年1月頃(今年は2012年1月17日～20日に開催)
  - 開催場所:マイアミ
  - 主　　催:DigitalBond
- 過去の講演内容
  - 制御システムに用いられるプロトコルに関する分析や脆弱性の公開
  - 制御システムでどのようにセキュリティ対策を行うかの調査

Copyright® 2012 JPCERT/CC All rights reserved.

Project Basecamp

- PLC に関するセキュリティ上の問題点が無いか調査

	A-B	Schneider Electric	GE	SEL	Koyo
Firmware	!	✗	!	!	!
Ladder Logic	!	!	✗	!	✗
Backdoors	!	✗	✗	✓	✓
Fuzzing	✗	✗	✗	!	!
Web	!	✗	N/A	N/A	✗
Basic Config	!	!	✗	!	!
Exhaustion	✓	✓	✗	✓	✓
Undoc Features	!	✗	✗	!	!

Copyright® 2012 JPCERT/CC All rights reserved.

- JPCERT/CCのこれまでの取組み
- JPCERT/CCのこれからの取組み
- 制御システム向けツールの紹介
- S4 Project Basecamp
- まとめ

Copyright® 2012 JPCERT/CC All rights reserved.

まとめ

JPCERT/CC 2012年の取組み

- インシデント対応に必要な技術および実態の調査
- ポータルサイト
- 制御システムセキュリティアセスメントツール
- セキュアコーディング
- 脆弱性ハンドリング

ツールの紹介

- 制御システム向けのセキュリティツールは公開済

S4

- 制御システムのみならず、制御装置自身もターゲットに

Copyright® 2012 JPCERT/CC All rights reserved.

お問い合わせ

- 制御システムセキュリティ

  連絡先：cs-security-staff@jpcert.or.jp

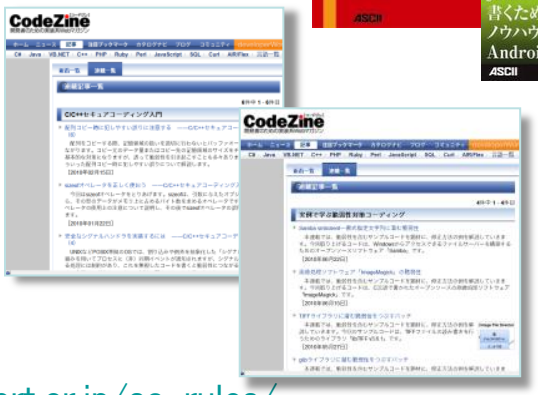
  H　　P：https://www.jpcert.or.jp/ics/

Copyright® 2012 JPCERT/CC All rights reserved.

お問い合わせ

セキュアコーディング

連絡先：secure-coding@jpcert.or.jp



- 書籍
  - —『C/C++セキュアコーディング』
  - —『CERT C セキュアコーディングスタンダード』
  - —『Java セキュアコーディングスタンダード　CERT/Oracle版』
- Web記事連載
  - CodeZine　－　C/C++セキュアコーディング入門
    http://codezine.jp/article/corner/339
  - CodeZine　－　Javaセキュアコーディング入門
    http://codezine.jp/article/corner/437
- その他
  - CERT C Secure Coding Standard 日本語版　http://www.jpcert.or.jp/sc-rules/
  - Java セキュアコーディングスタンダード CERT/Oracle 版　http://www.jpcert.or.jp/java-rules/
  - Java セキュアコーディング　並行処理編
    http://www.jpcert.or.jp/securecoding_materials.html#certjavacon
  - OWASP「ソフトウエアセキュリティ保証成熟度モデル
    http://www.jpcert.or.jp/securecoding_materials.html#owaspsamm
  - ソースコード解析ツールを活用したCERTセキュアコーディングルールの有効性評価報告書（英語版、日本語版）http://www.jpcert.or.jp/research/Analysistools.html

Copyright® 2012 JPCERT/CC All rights reserved.

ご静聴ありがとうございました。

JPCERTコーディネーションセンター

— Email：office@jpcert.or.jp

— Tel：03-3518-4600

— Web: http://www.jpcert.or.jp/

Copyright® 2012 JPCERT/CC All rights reserved.