

# PLANT \* CML<sup>®</sup>

an EADS North America Company

## 2009 VULNERABILITY ASSESSMENT

### SECURITY STATEMENT

RESTRICTED DISCLOSURE

DECEMBER 29, 2009  
Release 1.2



**Deliverable Accuracy Certification**

nGuard Audit QA: Jim Brown, CISSP

Signature: Jim Brown

Date: 01/22/2010

3700 Arco Corporate Drive, Suite 525  
Charlotte, North Carolina 28273  
704-583-4088 phone  
704-973-9298 fax

---


## Table of Contents

Project Contacts & Confidentiality .....	ii
Plant*CML Contact(s) .....	ii
nGuard Contact(s) .....	ii
Confidentiality Statement.....	iii
Security Statement.....	1
Project Overview.....	1
Audit Firm Background .....	1
Summary.....	4

## Project Contacts & Confidentiality


**Plant\*CML  
Contact(s)**

The following table lists pertinent Plant\*CML contact information for this project:

 <i>an EADS North America Company</i>	
Name	Title
Christina Lupton	Managed Services Manager
Kevin Cox	Sr. Solutions Architect
David Park	Managed Services System Analyst

**nGuard  
Contact(s)**

The following table lists the pertinent nGuard contact information for this project:

		<b>nGuard</b> 3700 Arco Corporate Drive, Suite 525 Charlotte, North Carolina 28273 704-583-4088 phone 704-973-9298 fax
Name	Title	Contact Information
Eric Waddell, CISSP, GCFW, PCI QSA, CCNA	Principal Engineer	Mobile Phone: 704.813.4062 Main Phone: 704.583.4088 x8003 E-mail: eric.waddell@nGuard.com
Devin Hogan	Security Engineer	Mobile Phone: 704.995.4987 Main Phone: 704.583.4088 x8008 E-mail: devin.hogan@nguard.com
Jim Brown, CISSP	Principal Consultant	Mobile Phone: 704.651.1014 Main Phone: 704.583.4088 x8001 E-mail: jim.brown@nguard.com
Marty Burks	Account Executive	Mobile Phone: 704.516.8592 Main Phone: 704.583.4088 x8005 E-mail: marty.burks@nguard.com

---

**Confidentiality  
Statement**

This document is the exclusive property of Plant\*CML and nGuard. This document contains proprietary and confidential information and may not be duplicated, redistributed, or used, in whole or in part, in any form, without the written consent of both Plant\*CML and nGuard.

---

---

## Security Statement

---

### **Project Overview**

In the third quarter of 2009, the management team of PlantCML Managed Services authorized a security audit and selected nGuard, Inc. to conduct the audit activities. These audit activities began in September 2009 and were completed in December of 2009.

As an independent security assessment firm, nGuard conducted the audits in accordance with generally accepted information security best practices. Performed by credentialed security professionals, we believe that our audits provide a reasonable basis for our opinion on the security posture of the audited systems and infrastructure.

---

### **Audit Firm Background**

#### **Proven**

Based in Charlotte, NC, nGuard is a highly focused security assessment firm. nGuard is led and staffed by industry veterans with a proven track record. nGuard's heritage traces back to 1994 when the core group of nGuard's senior security professionals founded the security practice of a major regional integration firm. Today, our team is comprised of highly experienced and credentialed security professionals with decades of aggregate, real-world experience.

#### **Longevity**

The nGuard team's longevity in the market place is well known in the Southeast:

- nGuard has current clients that have worked with the nGuard team since 1992.
  - The management team has been working together for the past 16 years.
  - nGuard's assessment engineers and consultants have the essential experience and security certifications required and recognized by auditors.
- 

### **Expertise**

nGuard staffed this assessment with highly experienced and seasoned security professionals. The assessment team's credentials are summarized below:

- Over 60 years aggregate security experience
- Experienced in providing all assessment options that have been proposed
- Since 1994, team members have conducted a broad variety of security assessments across a diverse clientele, ranging from small regional firms to Global 500 companies
- Have delivered specialized security assessments for clientele striving for compliance with regulating federal agencies
- The lead assessment engineer for this engagement has thirteen years of information security experience and holds a variety of

security certifications including:

- Certified Information Systems Security Professional (CISSP – since 2001)
- Payment Card Industry Qualified Security Assessor (PCI-QSA)
- Global Information Assurance Certification Gold (GCFW-Gold)
- IRCA ISO 27000 Auditor

### Rating Summary

Upon completion of assessment and analysis activities, nGuard was able to establish the following ratings for the various audit areas.

Audit Area	Rating
Internet Perimeter	4.0
Internal Network	4.0
Web Application	4.0
Database Audit	4.0
Dial-Up Audit	4.0

The Audit Area scoring is a **subjective** measurement based on compliance with security best practices and the evaluation of the assessment team. Here is a short description of the various ratings, from most favorable to least favorable.

Rating	Description
4	Subject area represents industry best-practice.
3	Subject area performed well in most areas but requires improvement.
2	Subject area performed well in some areas and requires significant improvement in others.
1	Subject area was significantly deficient and requires immediate focus on remediation of the key issues.

### Audit Activities

nGuard performed the following audit activities in the course of this engagement.

**Internal Vulnerability Testing.** nGuard conducted a focused assessment of PlantCML Managed Services' internal networks and systems including activities such as service mapping, vulnerability mapping, automated and manual exploitation. nGuard examined this infrastructure for the presence of different vulnerabilities numbering in the thousands.

**Score:** 4.0 out of 4.0

**Summary:** nGuard has tested the Internal security posture and found that only minor vulnerabilities currently exist. Furthermore, as of the date of

this statement, no exploitable vulnerabilities were discovered that would allow an attacker unauthorized access to sensitive data.

---

**Web Application Testing.** nGuard conducted a focused assessment of PlantCML Managed Services' web applications including activities such as cross-site scripting, username/password harvesting, brute force logins, SQL and blind SQL injection, and user access control circumvention. nGuard examined applications for the presence of thousands of known vulnerabilities as well as unknown application specific custom vulnerabilities.

**Score:** 4.0 out of 4.0

**Summary:** nGuard has tested the application security posture and found that no exploitable vulnerabilities currently exist. Furthermore, as of the date of this statement, no vulnerabilities were discovered that would allow an attacker unauthorized access to sensitive data or systems.

---

**Database Vulnerability Testing.** nGuard conducted a focused assessment of PlantCML Managed Services' databases including testing of specific vulnerabilities that exist in the way databases interact with users and other applications. The auditing focused on areas such as database authentication and authorization, and potential information leaks.

**Score:** 4.0 out of 4.0

**Summary:** nGuard has tested the application security posture and found that no exploitable vulnerabilities currently exist. Furthermore, as of the date of this statement, no vulnerabilities were discovered that would allow an attacker unauthorized access to sensitive data or systems.

---

**Dial-up Vulnerability Testing.** nGuard conducted a focused assessment of PlantCML Managed Services' analog phone extensions. Each accessible number was dialed and connected to in order determine if the end system was phone, fax, or modem connected to a computer system. Systems found answering were then subjected to attacks such as brute force authentication, common credentials, as well as hundreds of known attacks against dial-up modems.

**Score:** 4.0 out of 4.0

**Summary:** nGuard has tested the dial-up security posture and found that no exploitable vulnerabilities currently exist. Furthermore, as of the date of this statement, no vulnerabilities were discovered that would allow an attacker unauthorized access to sensitive data or systems.

---

---

**Summary**

nGuard found that in all areas of audit activity that PlantCML Managed Services were properly maintaining a secure computing environment that appropriately protects the information and systems from unauthorized access and control.

*NOTE: The audit scores and findings are based on a "snapshot in time" specific to the timeframe in which the audit were conducted and makes no guarantee on the ongoing security posture of the audited networks and systems.*

---



Last Page