SAINTwriter Assessment Report

Report Generated: July 27, 2010

1.0 Introduction

On March 11, 2010, at 2:23 PM, a web crawl vulnerability assessment was conducted using the SAINT 7.3 vulnerability scanner. The web directories and CGI pages which were detected during the scan are presented in the following sections.

2.0 Overview

The following vulnerability severity levels are used to categorize the vulnerabilities:

CRITICAL PROBLEMS
Vulnerabilities which pose an immediate threat to the network by allowing a remote attacker to directly gain read or write access, execute commands on the target, or create a denial of service.

AREAS OF CONCERN
Vulnerabilities which do not directly allow remote access, but do allow privilege elevation attacks, attacks on other targets using the vulnerable host as an intermediary, or gathering of passwords or configuration information which could be used to plan an attack.

POTENTIAL PROBLEMS
Warnings which may or may not be vulnerabilities, depending upon the patch level or configuration of the target. Further investigation on the part of the system administrator may be necessary.

SERVICES
Network services which accept client connections on a given TCP or UDP port. This is simply a count of network services, and does not imply that the service is or is not vulnerable.

The following tables present an overview of the hosts discovered on the network and the vulnerabilities contained therein.

2.1 Host List

This table presents an overview of the hosts discovered on the network.

Host Name	Netbios Name	IP Address	Host Type
10.7.0.2		10.7.0.2	Windows 2000 SP2

2.2 Vulnerability List

This table presents an overview of the vulnerabilities detected on the network.

Host Name	Vulnerability / Service
10.7.0.2	Web Directory: /
10.7.0.2	Web Directory: /cgi-bin/