External Vulnerability Assessment

-Executive Summary-

Prepared for:

ABC ORGANIZATION

On

March 9, 2008

Prepared by:

AOS Security Solutions
# Table of Contents

**Executive Summary** ........................................................................................................................................... 3  
  Immediate Focus Areas (1-4 weeks) .................................................................................................................. 3  
  Short term Focus Areas (1-6 months) .................................................................................................................. 3  
  Long term Focus Areas (6 months +) .................................................................................................................. 3  

**Web Application Assessment Statics** ........................................................................................................... 4  
  Items of Top Concern: ........................................................................................................................................... 4  
  AOS Recommendations: ....................................................................................................................................... 4  

**Network & Service Vulnerability Assessment** ............................................................................................... 5  
  Items of Top Concern: ........................................................................................................................................... 5  
  AOS Recommendation: ......................................................................................................................................... 5
Executive Summary
Alexander Open Systems (AOS) performed an external security vulnerability assessment of ABC ORGANIZATION. An external assessment looks devices such as firewalls, servers and routers that provide services on the Internet. It also covers application layer assessments on any web based services externally facing.

The security assessments performed by Alexander Open Systems, Inc follow a standard assessment methodology beginning with reconnaissance, vulnerability enumeration and penetration testing for validation. AOS performs these assessments with the least possible impact to the organization. This means our assessment tools have been throttled back as to not consume customer Internet bandwidth. Our assessments are also done at a mutually agreeable time which is determined to be least impacting to the organization. The following sections are the findings of AOS’s vulnerability assessment services.

Immediate Focus Areas (1-4 weeks)
ABC ORGANIZATION should take immediate action in the resolution of vulnerabilities found on the web server ([http://zero.webappsecurity.com](http://zero.webappsecurity.com)). Security holes on this system have been found that put the organization in direct risk. The AOS recommendation to immediately solve this risk is to layer the web server with an application layer firewall.

Short term Focus Areas (1-6 months)
ABC ORGANIZATION needs to review the current certified operating system levels and upgrade systems not holding true to that standard. A patch management system (if not currently deployed) should be deployed for all high risk assets in the organization. For systems that cannot be patched or rebooted in a timely manner yet still holding key assets, AOS recommends a host based intrusion prevention system to adequately protect those systems from both known and unknown attacks.

Long term Focus Areas (6 months +)
ABC ORGANIZATION needs to audit application development. A strong emphasis on application security needs to be stressed and all custom applications should have a vulnerability assessment done prior to implementation into production environments.

Ongoing application and network assessments should also be done to ensure current systems don’t become vulnerable to new security threats

Vulnerabilities found on ([http://zero.webappsecurity.com](http://zero.webappsecurity.com)) in regards to application coding should be resolved and tested/verified.
Web Application Assessment Statics

The graph below displays the vulnerabilities that were found on http://zero.webappsecurity.com/. These represent the risk to the server, the data it contains and ultimately risk to ABC ORGANIZATION. Items categorized in the below graph show vulnerabilities in the application itself.

![Vulnerabilities by Severity]

**Items of Top Concern:**

In the above graph, several critical level vulnerabilities were found. Of the number of vulnerabilities found the three top security risks have to deal with:

- SQL Injection
- Cross Site Scripting
- Information Leakage

**AOS Recommendations:**

Due to the quantity and type of vulnerabilities found on the web application, Alexander Open Systems recommends layering the web site with an application layer firewall as well as restricting access to specific areas of the server.
Network & Service Vulnerability Assessment

The graph below displays the number of security related vulnerabilities found on the external facing network of ABC ORGANIZATION. These vulnerabilities were found from various tools that were focused at finding security weaknesses in the system or service level security protections.

Items of Top Concern:
There was one high level security vulnerability on the external network and it can be resolved by a system patch. If exploited, this vulnerability will cause the server to continuously reboot impacting both the availability and integrity of the data contained on the system.

AOS Recommendation:
System patches are generally the number one security risk we see on internal systems to date. Typically, internal threats come from poor system patch management on internal devices. In addition, system patches are generally not applied until after the system reboots. This makes it difficult to apply patches to production facing systems that must maintain a high level of uptime. AOS generally recommends a combination of good patch management with host based intrusion prevention. HIPS, or host based intrusion prevention, allows system administrators the time they need to effectively test, certify and deploy system patches while not putting business assets at risk.