

DataSheet

AlertSite Security Vulnerability Scan with PCI

Because of the increasing severity of security intrusions and identity theft, companies are vulnerable to malicious attacks even with firewalls, anti-virus and penetration safeguards in place. **Secure your web sites** and servers before intruders attack. AlertSite's Security Vulnerability Scan **identifies over 14,000 vulnerabilities** in real-time, categorizes the risks and then provides recommendations and solutions. Our powerful, up-to-date and easy-to-use remote security scan ensures your web sites, servers, firewalls and Internet-connected devices are free of known vulnerabilities. AlertSite partners with Sunera, a leading provider of risk and controls consulting services, to provide a complete **PCI compliance and security scanning solution**, enabling merchants and credit card service providers to achieve and maintain PCI compliance.



Scan from
outside
the firewall.

Scan Internet
devices, services,
ports, routers and
firewalls daily.

No software to
install, configure
or maintain.

Maintain PCI
Compliance.

d e m a n d p e r f o r m a n c e

PCI Compliance Scan

AlertSite PCI services help merchants and service providers achieve PCI Compliance. Components of the compliance process include:

- Network scans.
- On-site audits.
- Report on compliance.
- Gap analysis.
- Self-assessment questionnaire assistance.
- Remediation and integration with operations.

Other Information Security Capabilities

AlertSite, together with Sunera, offers additional security services including:

- Vulnerability assessment.
- Risk assessment.
- Web application security assessment.
- Physical security assessment.
- Penetration testing.
- Wireless security.
- Comprehensive training and education.

Infrastructure Design, Deployment and Hardening

Whether you want to re-engineer your infrastructure, deploy an IDS solution or simply “harden” existing systems, our engineers have the skills to assist you. Our services include:

- Feasibility studies.
- Product selection.
- Rules and policy development.
- Network re-engineering.
- Installation and configuration.
- Development of Report and Analysis template.
- Post-implementation security testing.
- Performance tuning.

Related security services include:

- Sarbanes-Oxley section 404 assistance.
- ERP controls and integration services.
- Penetration studies and internal network/vulnerability assessments.
- HIPAA, GLB and California privacy legislation compliance assessments.
- Security program, policies, procedures and standards development.
- Identity management and single sign-on deployment.
- Internal audit services.
- IT audit services.

PCI Report

PCI Report

ID	Finding	Severity	Recommendations
U1	MySQL-GQL (/430f2c) - The Administrator (SA) password on the remote database is blank and/or 'sa'	Open	Configure the Administrator account to require a complex password that is frequently changed.
U2	MySQL-GQL (/430f2c) - Missing critical patch which could be exploited by an attacker to gain SYSDBA access on the host.	Open	Install MySQL patch. For more information, see http://www.mysql.com/securehotfixes/mysql-5.1.58-1.html .
U3	Oracle Web Services - The remote host is using a version of OracleDB, which is older than 8.0.60 or 8.1.7.4. The remote host is using a version of oracle_oci which is older than 2.8.16.	Open	OracleDB: upgrade to version 8.0.60 or 8.1.7.4 or newer oracle_oci: upgrade to version 2.8.16 (Apache 1.3) or to Apache 2.0.33
U4	IIS Server (/110f2c) - This host seems to be running an IIS server, but the IIS server responds to an empty query with a 404 error. This behavior may be indicative of an IIS bot, worm, or other virus infection. It is only likely the system has been compromised or is	Open	Reinstall or remove from operation

ID	Finding	Severity	Recommendations
U5	Apache Web Services - The remote host appears to be running a version of Apache which is older than 1.3.29 or 2.0.18.12.10.12.10	Open	There are several flaws in this version, which may allow an attacker to disable the remote server remotely. Upgrade to the latest version.
U6	DNS - DNS Servers allow recursive queries. DNS cache poisoning and spoofing. Denial of Service attacks against other networks can be performed against DNS servers that allow recursive queries.	Open	Review DNS Server configuration and alter configuration to deny recursive queries. Review additional information related to this issue at http://www.cis.ohio-state.edu/secure/CIS_7397-02.html .
C1	Web Management Portal - The remote web servers are affected by buffer overflow vulnerability.	Open	The remote host is running a Compaq Web Management Server. The remote version of this software is vulnerable to an unauthenticated buffer overflow that may allow an attacker to execute arbitrary code on the remote host with the privileges of the web server process. See also: http://www.securityfocus.com/bid/10047
C2	MySQL SQL Appliance - The following MySQL appliance is vulnerable to SQL injection techniques.	Open	An attacker may exploit these flaws to bypass authentication or to take the control of the remote database. Modify the relevant CGI so that they properly restrict arguments. See also: http://www.securityfocus.com/bid/10047
C3	Microsoft IIS Server - Multiple missing critical patches and default configurations. An attacker may exploit these IIS servers in a bot farm or exploit it as a result of an attacker may use known issues in a backdoor attack to gain user usernames and passwords.	Open	Install critical Microsoft patches. See also: http://www.microsoft.com/securehotfixes/MS04-028.aspx Remove default settings that are not used: http://www.microsoft.com/secure/MS04-028 Disable or restrict the use of .ht files

The PCI Compliance Reports assign a severity rating, provide a description for, and suggest recommendations for each vulnerability identified.

AlertSite is a recognized leader in security vulnerability scanning services and PCI Compliance solutions.

AlertSite is a leading provider of web performance measurement, systems monitoring and security vulnerability scanning products that ensure a customer's critical web-based services are always available and running at peak performance. AlertSite's range of hosted Internet services benefit all types and sizes of businesses and organizations.

Our global monitoring network keeps watch for you.

Founded in 1998, AlertSite is based in South Florida and maintains 30 global monitoring stations in highly qualified data centers on every continent but Antarctica. Our global network monitors the availability and performance of your web site and web-based applications and transactions wherever they are operating across the globe. When trouble occurs, AlertSite helps you isolate the location of the problem.

AlertSite Control Panel



Our Performance Advisors are ready to serve you.

An important difference between AlertSite and our competition is the availability and skill of our Performance Advisors. These highly trained technical experts are always available live from 8:00 a.m. to 6:00 p.m, EST, Monday through Friday. We also offer on-call support through 9:30 p.m, EST. AlertSite's Performance Advisors can help you get the most out of your AlertSite applications, as well as interpret security issues that may affect you.

Join our more than 2,000 customers.

With more than 2,000 satisfied AlertSite customers across virtually every industry around the world, you'll be in good company. We count among our clients some of the biggest names, including AT&T, Circuit City, Honda, Intel, Symantec and many others, all of whom put their trust in AlertSite's proven portfolio of hosted services.

If you are not yet a member of the AlertSite customer family, we invite you to contact us today for a complimentary, no-obligation assessment of your web site requirements. Call 877.302.5378 now, or go to www.AlertSite.com to sign up for your free trial immediately.

The AlertSite Control Panel is your starting point for all AlertSite reports and diagnostics. The Control Panel has an automatic refresh, which provides an up-to-the-minute view of site performance.

877.302.5378

www.AlertSite.com