



ACI – Third-Party Software Vulnerability Tracking Process

Who is ACI?

ACI is a software product and services company

- In business since 1975
- 30+ products mostly dealing with financial transactions
- 2000+ employees worldwide
- 800+ customers in 88 countries
- Last year – 80 billion consumer payment transactions
- Estimate \$5 trillion in wholesale payments per day

Why Track Third-Party vulnerabilities?

PCI Requirement

- PCI-DSS v1.1 section 6.2
- PABP v1.4 section 7.1

Risk Management

- Customers may not test third-party patches
 - Don't want system outage
 - Attackers exploit these vulnerabilities in hopes that system updating is slow.
- Proactive position with regards to notification

Good Business

Third-Party Software

Operating Systems

- Guardian, HP-UX , AIX, OS/390, z/OS, Windows

Middleware

- Databases
 - C-Tree, Enscribe, VSAM, SQL Server, Oracle, DB2
- Messaging
 - WebSphereMQ
- Web Application Server
 - Tomcat, WebSphere, WebLogic
- HTTP Server
 - Apache, IIS

Java SDKs, JVMs

Libraries, including open-source

Third-Party Vulnerability Tracking Participants

Security Engineering

- Overall support of system
- First level filtering for false positives

Product Lead

- Document dependency on third-party products
- Second level filtering for false positives
- Testing of third party patches with current release
- Forward issues to Product Development
- Inform Customer Management of status

Product Development

- Provide product fixes
- Notify Product Lead when complete

Customer Management

- Notify Customers of vulnerabilities and fixes

Third-Party Tracking Process

ACI Subscribes to Symantec DeepSight Alert Service

The screenshot displays the Symantec DeepSight Alert Services web interface within a Microsoft Internet Explorer browser window. The browser's address bar shows the URL <https://alerts.symantec.com/ViewMyAlerts.aspx>. The page title is "Symantec DeepSight Alert Services".

The interface includes a navigation menu on the left with options: Home, View Alerts, Configure Alerts, User Profile, and Administer Users. The main content area is titled "View Alerts" and features a search bar and a "Go" button. Below this, there are tabs for "My Alerts", "All Alerts", "Advanced Search", and "Alerts Reporting".

The "My Alerts" section contains a "Date Range" filter with "From" set to 1/1/2008 and "To" set to 5/17/2008, and an "Alert Type" dropdown menu set to "All Types". There are "Submit" and "Reset" buttons. A table below shows a list of alerts, with 10 records displayed per page.

	Title	Delivered	Type
N/A	Perl Unicode Regular Expression Buffer Overflow Vulnerability	2008-02-21 20:13:09Z	Vulnerability
N/A	Perl Unicode Regular Expression Buffer Overflow Vulnerability	2008-02-20 16:58:08Z	Vulnerability
N/A	Mozilla Firefox/Thunderbird/SeaMonkey Chrome-Loaded About:Blank Script Execution Vulnerability	2008-02-19 22:28:31Z	Vulnerability
N/A	Multiple Browser URI Handlers Command Injection Vulnerabilities	2008-02-19 22:28:31Z	Vulnerability
N/A	Mozilla Firefox 2.0.0.4 Multiple Remote Vulnerabilities	2008-02-19 22:23:10Z	Vulnerability
N/A	Mozilla Firefox 2.0.0.7 Multiple Remote Vulnerabilities	2008-02-19 22:18:05Z	Vulnerability
N/A	Sun Java WebStart Multiple File Access And Information Disclosure Vulnerabilities	2008-02-19 22:03:02Z	Vulnerability
	Sun Java Runtime Environment Multiple Weaknesses	2008-02-19 21:58:04Z	Vulnerability
N/A	Sun Java Runtime Environment Virtual Machine Remote Privilege Escalation Vulnerability	2008-02-19 21:48:02Z	Vulnerability
N/A	Apache HTTP Server Worker Process Multiple Denial of Service Vulnerabilities	2008-02-18 15:43:02Z	Vulnerability

At the bottom of the table, it indicates "Page: 1", "Total Pages: 10", and "Total Records: 100". There are also navigation buttons for the table pages.

DeepSight Configuration

A new “Technology” is added for each ACI product

The screenshot shows the Symantec DeepSight Alert Services web application in Microsoft Internet Explorer. The browser address bar shows <https://alerts.symantec.com/TechLists.aspx>. The page title is "Symantec DeepSight Alert Services". The navigation menu includes Home, View Alerts, Configure Alerts (selected), User Profile, and Administer Users. The main content area is titled "Configure Alerts" and has tabs for "Configure Monitors", "Tech Lists" (selected), and "Delivery Methods". A search box is present. Below the tabs is a "Technology Lists" section with a dropdown menu set to "10". The table below lists various technologies with their attributes and actions.

Name	Attributes	Actions
All Technologies		Configure View Duplicate Delete
BASE24-eps	S C	Configure View Duplicate Delete
Dispute Management System	S C	Configure View Duplicate Delete
Firewalls	S C	Configure View Duplicate Delete
Money Transfer System	S C	Configure View Duplicate Delete
Open2	S C	Configure View Duplicate Delete
Payments Manager	S C	Configure View Duplicate Delete
Proactive Risk Manager	S C	Configure View Duplicate Delete
Retail Commerce Server	S C	Configure View Duplicate Delete
Smart Chip Manager	S C	Configure View Duplicate Delete

Page: 1 Total Pages: 1 Total Records: 10

DeepSight Configuration (cont.)

Third-Party Software is monitored for each “Technology”.

Configure Alerts Search

Configure Monitors **Tech Lists** Delivery Methods

Technology List Configure

Switch To

Technology List Name (max 50 chars): [Technology List Help](#)

Search By: Search Text:

Category	Vendor	Product	Versions
Email	IBM	AIX	4.3.0
Games	Immunix	iSeries AS400	4.3.1
Instant Messaging	Ingate	Microsoft Windows XP	4.3.2
Multimedia	iPod Linux Project	MVS	4.3.3
Networking	Juniper Networks	OS/2	5.1
Operating Systems	Knoppix	OS/390	5.1.0 L
Printing	Kondara	OS/400	5.2
SCADA	Linksys	OS/400 V5R3M5	5.2.0 L
Security	Linux	TotalStorage DS400	5.2.2
Server	Lucent	z/OS	5.3
System	LynuxWorks	z/VM	5.3.0 L
Top 100 Technologies	MandrakeSoft		5200-10
Unknown/Other	Marconi		5300-06
Web	McDATA		6.1

Inclusions **Exclusions**

DeepSight Configuration (cont.)

Email Alerts are Forwarded for Each Reported Vulnerability

Symantec DeepSight Alert Services - Microsoft Internet Explorer

Address: <https://alerts.symantec.com/DeliveryMethodConfigure.aspx?id=33278>

symantec. DeepSight™ Alert Services Documentation Help Logou

Home
View Alerts
Configure Alerts
User Profile
Administer Users

Configure Alerts Search

Configure Monitors Tech Lists **Delivery Methods**

Delivery Method Configuration

Switch to: Sec Engr Delivery Method Edit

Delivery Method Type: email

Delivery Method Name: Sec Engr Delivery Method

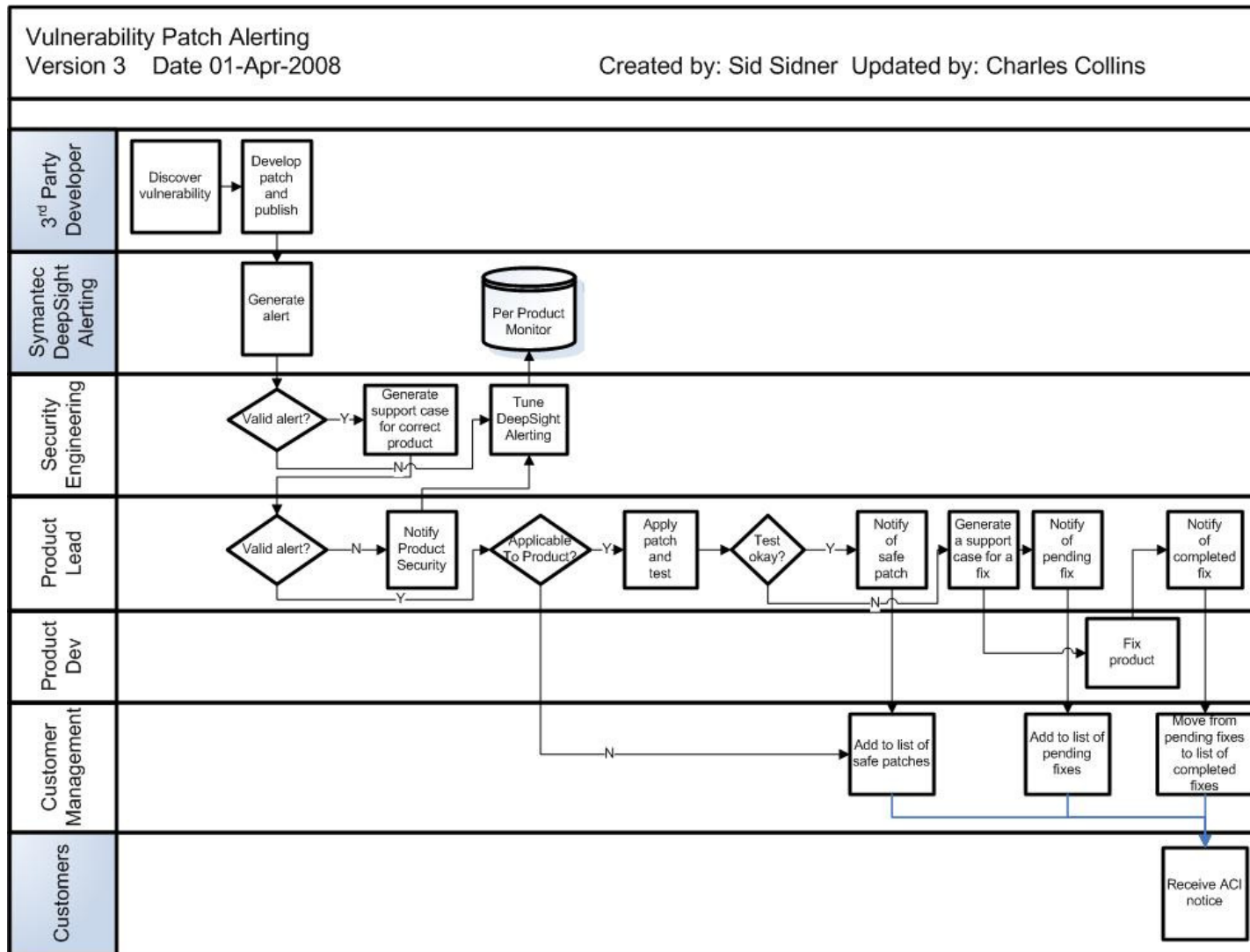
Address or Number: Charles.Collins@ACIWorldwide.com

Save Cancel

E-mail If you select this delivery method type, alert messages will be delivered to you via electronic mail. E-mail alerts can be any detail level you choose, and can be anywhere from a few hundred characters to a few pages long. Enter your e-mail address in the Address or Number input field. Example: john.doe@example.com

Internet

Vulnerability Tracking Process Flow





EVERY SECOND. EVERY DAY.