ALCATEL-LUCENT ENTERPRISE SECURITY STRATEGY

DESCRIPTION OF THE SECURITY FLAW REMEDIATION PROCESS

STRATEGIC WHITE PAPER

PRODUCT AND OFFER MANAGEMENT
JUNE 2012

TABLE OF CONTENTS

SECURITY AS A PROCESS

All business requirements for security technology should be focused on delivering appropriate and not excessive security. Based on these assumptions, internal Alcatel-Lucent security processes and frameworks have been defined at both the corporate level and the business unit level.

In the Enterprise Business Group for data and voice solutions, Alcatel-Lucent has developed a strategy called the user-centric approach to security.

Alcatel-Lucent offers a coherent, comprehensive security strategy to respond to the diverse challenges associated with networks, mobile technologies and business applications. By building security into the way you work, you can be confident that your business is built on firm foundations.

User-centric security is about answering people's needs in ways that preserve the integrity of the enterprise network and its assets. User security can almost seem like protecting the network from the user — securing it against vulnerabilities that user needs introduce. For user-centric security to be realized, enterprises must create a secure environment within which end users can go about their business.

In addition to this strategy, Alcatel-Lucent has created processes to distribute, to its business partners and customers, software fixes in case a vulnerability is discovered in an Alcatel-Lucent product.

> "Security is a process and not a product. Products provide some protection, but the only way to effectively do business in an insecure world is to put processes in place that recognize the inherent insecurity in the products."
>
> Bruce Schneier,
> described by The Economist
> as a security guru

ALCATEL-LUCENT SECURITY PRACTICE

Security is not only a set of features in a product but also a continuous process to track vulnerabilities. The vulnerability landscape is evolving every day; the most secure product today can be vulnerable tomorrow because new attacks could be discovered.

At the Alcatel-Lucent corporate level, the Incident Response Team receives vulnerability alerts from business partners, customers and Cert-IST (Computer Emergency Response Team - Industry, Services and Tertiary).

Alcatel-Lucent is a founding and active member of Cert-IST, which is one of three French Certs and a member of the worldwide network of Certs, the global Forum for Incident Response and Security Teams (FIRST, http://www.first.org/).

With experience gathered since 1994, the Alcatel-Lucent Security Practice ensures Cert-IST services (http://www.cert-ist.com/eng/presentation/HistoriqueduCertIST/).

Alcatel-Lucent ensures that proper actions are taken at the product line level to analyze vulnerabilities, evaluate the impact on products, fix security problems and inform business partners and customers.

The Incident Response Team forwards the alerts to the group of security experts in the applicable business group for analysis. The security group in the Enterprise Business Group is composed of Research & Development (R&D) personnel, a product architect and a product line manager. If one or both products of the IP Telephony solution (Alcatel-Lucent OmniPCX™ Enterprise Communication Server or Alcatel-Lucent OmniPCX™ Office Rich Communication Edition) or the Unified Communications solution (Alcatel-Lucent OpenTouch™ Conversation) is impacted, corrective actions are taken to resolve the issue and workarounds are provided when possible to reduce risk before a fix is available.
The final communication is done through business partners, who inform their customers about vulnerabilities, workarounds and resolutions.

GENERAL PROCESS FOR HANDLING CUSTOMER SERVICE REQUESTS

The general process for handling customer service requests is:

1. An end customer identifies a defect and transmits it to their business partner.
2. The business partner addresses the defect (for example, if it is a configuration-related issue) or opens a service request (SR). SRs are tracked using a customer relationship management tool that business partners have access to, so they can open the SR themselves. Alternatively, customers and business partners can call an Alcatel-Lucent Support Center, and Alcatel-Lucent personnel will enter a new SR into the database.
3. The Alcatel-Lucent Support Center forwards the SR to the Technical Support Service.
4. The Technical Support Service analyzes the SR and does one of the following:
   - Closes it immediately (for example, by providing additional guidance to the business partner
   - Starts investigating the problem
   - Escalates the SR as a product flaw to R&D

1. The security flaw remediation process

The security flaw remediation process is implemented at two levels:

- The corporate level across the complete Alcatel-Lucent portfolio
- The product line level

At the corporate level

Our Quality Assurance and Customer Care central organization hosts the corporate-wide Alcatel-Lucent Portfolio Security Issue Response Team (PSIRT), which receives, investigates and internally distributes security information related to Alcatel-Lucent products and solutions (see Figure 1).

PSIRT personnel are members of the Security and Reliability Group.

PSIRT is the main gateway between Alcatel-Lucent and the general public:

- All external input is centralized at PSIRT: input from CERT-US, CERT-IST, other mailing lists and user input from business partners and customers (email: psirt.security@alcatel-lucent.com)
- All communications to security organizations such as the various Certs and to the general public is done through PSIRT.

The PSIRT process is as follows:

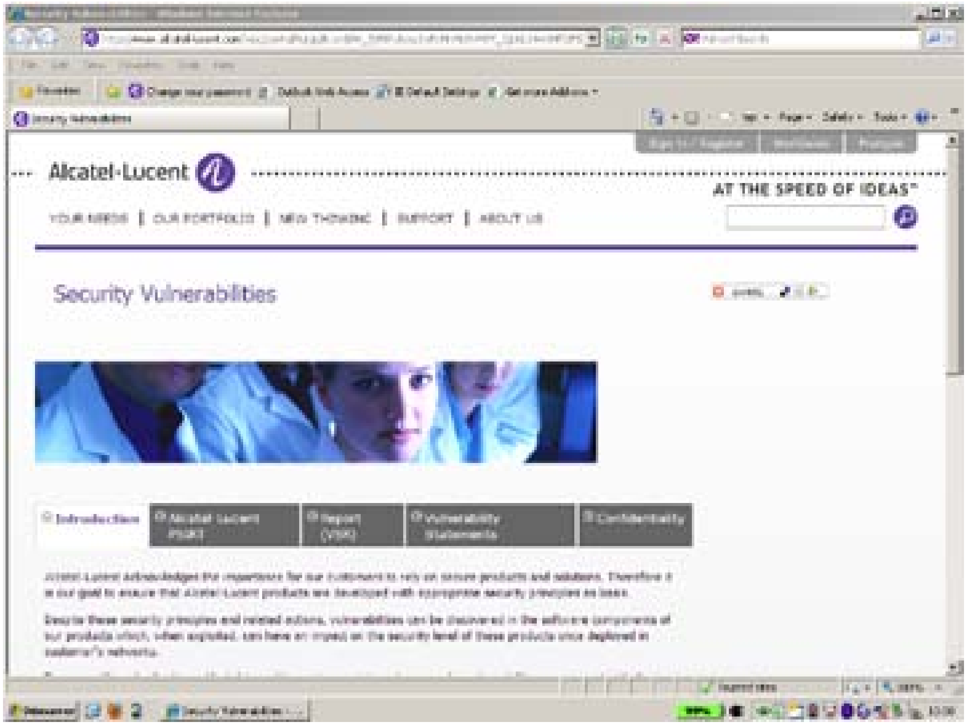
1. PSIRT receives and stores vulnerability reports, then distributes them internally to the relevant product groups’ contact persons, the Product Security Primes (PSPs).
2. The PSPs investigate the impact on their products and create detailed mitigation information and actions to be taken by business partners (for example, downloading a fix or upgrading the version of a product).

The PSIRT Coordinator supervises the process.

The centrally accessible internal vulnerability database (VDB) shown in Figure 1 lists all vulnerabilities for all products in the Alcatel-Lucent portfolio along with the status and response (workaround or fix from the PSPs) for each vulnerability. PSIRT personnel and PSPs can access the VDB.

The PSIRT Coordinator is automatically alerted of updates to the VDB made by the PSPs for each product. If the VDB has not been updated by a PSP, the PSIRT Coordinator sends an email request to the PSP for a specific status update.

Figure 1 shows the PSIRT web page.



Alcatel-Lucent acknowledges the importance for our customers to rely on secure products and solutions. Therefore it is our goal to ensure that Alcatel-Lucent products are developed with appropriate security principles as basis.

Despite these security principles and related actions, vulnerabilities can be discovered in the software components of our products which, when exploited, can have an impact on the security level of these products once deployed in customer's networks.

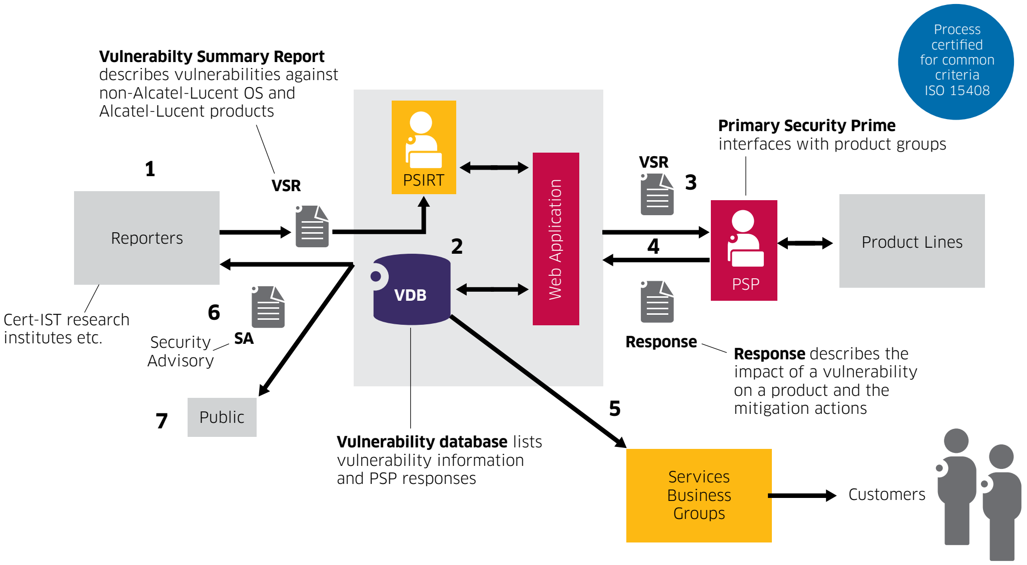
At the product line level

Each product is listed in PSIRT and has at least one identified PSP.

The PSP is responsible for:

- Analyzing the vulnerability reports (VRs)
- Creating a change request (CR) if the product is vulnerable
- Tracking the progress made toward correction of the vulnerability
- Ensuring that the expected service level agreement (SLA) for correcting vulnerabilities is achieved by raising the severity level of the vulnerability if required
- Forwarding the consolidated resolution to PSIRT
- Sharing with the product line groups the technical knowledge to correctly analyze and correct the vulnerability
- Explaining the resolution, which will be published on the Business Partner Web Site (BPWS). The product line groups decide which information to disclose to business partners. The complete PSIRT process followed by the Enterprise Products Group for its products, including the specific aspects linked to the indirect sales channel model, is shown in Figure 2

Figure 2. PSIRT process for Enterprise products


Process certified for common criteria ISO 15408
Vulnerabilty Summary Report describes vulnerabilities against non-Alcatel-Lucent OS and Alcatel-Lucent products
Primary Security Prime interfaces with product groups
1
VSR
Reporters
PSIRT
Web Application
VSR
3
PSP
Product Lines
2
VDB
4
Cert-IST research institutes etc.
6
Security Advisory
SA
Response
Response describes the impact of a vulnerability on a product and the mitigation actions
7
Public
5
Vulnerability database lists vulnerability information and PSP responses
Services Business Groups
Customers

Steps in the security flaw remediation process

1. An alert is received at the corporate level through one of these channels:

   Public PSIRT web site: http://www1.alcatel-lucent.com/psirt

   Email: psirt.security@alcatel-lucent.com

   Cert-IST vulnerability advisory
2. The PSIRT Coordinator enters the vulnerability into an internal alert database. This alert is numbered VU-yymmdd-# where yymmdd is the date when the alert is received and # is the alert arrival number on that day.
3. A vulnerability bulletin is emailed to the PSPs of all potentially vulnerable product lines.

   Product lines that are not vulnerable are automatically filtered out through a filter based on keywords specified by the PSPs. The PSPs are responsible for maintaining this filter.
4. The PSP analyzes the vulnerability bulletin and may reply with a verdict of Not Vulnerable.

   If the product is deemed vulnerable or if the PSP is unsure, the PSP opens a High Priority ticket in the product's database of defects to address the problem. (The other priority levels are Low and Normal.)

If the PSP needs more information to perform the analysis, he/she contacts the issuer of the alert (the discoverer or CERT-IST).

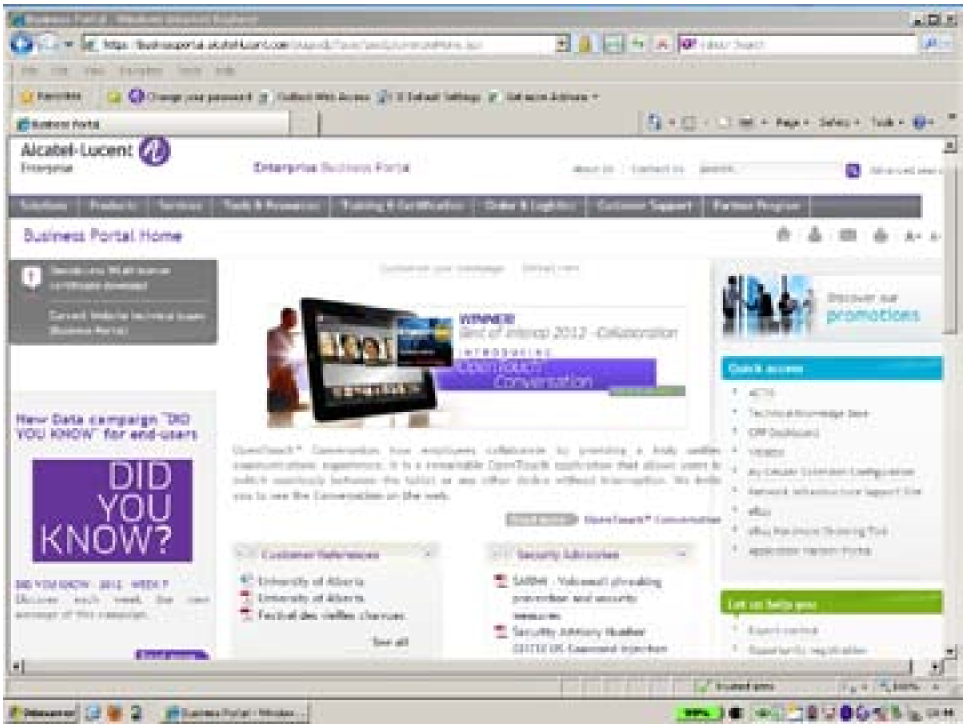
5. The PSP identifies, possibly with the help of product experts, a temporary workaround to mitigate the impact of this vulnerability. The workaround is published on the BPWS to enable the business partner to implement the workaround on the end customer's system at their earliest convenience. The workaround is called an Alcatel-Lucent Security Advisory (ASA).

6. The Product Maintenance Team develops a fix for the vulnerability and this fix undergoes quality assurance testing as specified in the product's development plan.

7. Technical Support Service publishes the fix on the BPWS. An update to the ASA is usually made to reflect the date the fix has been published.

Business partners are responsible for regularly visiting the BPWS, where new and updated ASAs are posted in the technical view of the BPWS home page (see Figure 3).

Figure 3. BPWS home page



A business partner reads an advisory to determine whether some of their customers are exposed to the vulnerability. If customers are affected, the business partner goes to the technical support section of the page (left menu) and downloads the fix for the product.

The business partner then determines with their customers when and how the fix can be deployed.

Once the fix is created by Technical Support, the PSP sends the PSIRT Coordinator an ASA containing information about this vulnerability that is of interest to the general public.

This ASA is published on the Alcatel-Lucent public security web site. The public advisory is also sent to Cert-IST for publication to their customers.

When the advisory is published on the public Alcatel-Lucent security web site, an email is automatically sent to everyone on the psirt.security@alcatel-lucent.com mailing list. Anyone may subscribe to this mailing list.

The security flaw remediation process has been examined as evidence during the standard certification process (ISO-15408) according to Common Criteria at assurance level EAL2+of the Alcatel-Lucent Communication Solution for Medium and Large Enterprises.

2. Summary of security flaw remediation process

1. Alert reporting through the PSIRT web site http://www1.alcatel-lucent.com/psirt

2. Alert disclosure to the general public by PSIRT on the public web site http://www1.alcatel-lucent.com/psirt following the established vulnerability disclosure policy. Disclosure to business partners is the responsibility of the product line groups within the Enterprise Product Group. Business partners then pass this information to end customers.

3. Alert processing by the relevant product line groups under guidance from the Medium and Large Enterprise (M&LE) committee, MLE-PSIRT, ensuring consistent analysis, information sharing and a prompt response.

3. Appendix: Template of the Alcatel-Lucent Security Advisory

The following template of the Alcatel-Lucent Security Advisory is published on the PSIRTweb site for Alcatel-Lucent business partners.

Alcatel-Lucent Security Advisory

No. SA0**XX** Ed. 01

Security Advisory CERT-IST/AV-2011.**XXX**
Vulnerability **XXX**

Summary

A vulnerability has been discovered in <**product**>.
It impacts <**product’s function**>.

Other references

Alcatel-Lucent defect number crms **XXXXX**

Affected products

<**OmniPCXOffice/OmniPCXEntreprise/OmniTouch/OTUC/ACAPI/AudioStation**>
release **Rn.x**

Description of the vulnerability

<**Precise description in the product’s context**>

Impacts

<**impact description specifically in the product’s context**>

Software versions and fixes

<**Product Rn.**j>: install patch **???** (available week **??**)
<**Product Rn.i**>: upgrade to release **Rn.j**
<**Product Rn.g**> and earlier: those releases are phased out: upgrade to release **Rn.j.**

Workarounds

<**None or description of the workaround**>

History

Ed.01 (**XXX**2011): creation