RUS CERT

CAIF

Common Announcement Interchange Format

http://CERT.Uni-Stuttgart.DE/projects/caif/

overview

- Introduction
- Project history
- Motivation
- Features
- Terminology: Types of Announcements
- Markup
- Text Structuring
- Text Containers
- Standard Sections
- Caif Users

CAIF

- proposal for a standard format of security announcements including but not limited to “advisories”
- XML-based
- intended to allow exchange according local policies
- flexibility by extensibility

Project History

- project started in 2OO2
- draft on requirements was issued in January 2OO3
- draft on format was issued in February 2OO4
- major update of format in May 2OO4, new DTD is online, draft yet to be updated
- prototype for new format operational

Motivation

- Due to the way information technology is deployed, security flaws are and will be a threat to the operation of IT infrastructure
- informing users and administrators about the problems is a vital task for vendors and security teams
- the common way to do so is the "security advisory"

Motivation

- many different Formats in use
  - different structure
  - different terminology
  - different assessment
- poor comparability

Motivation

- situation causes multiplication of work
- reusing advisories is difficult
- multiple re-writing tends to introduce errors
- descriptions may be constituency-dependent
- projects like CVE mitigate parts of the problem: they ease the

Conclusion

- A common format should
  - reflect the needs of readers
  - reflect the needs of issuers and authors
  - allow co-operation and re-usage
  - support automation of processes
  - be easily extended

Reader Requirements

- Typically the reader needs answers to the following questions:
  - Is the announcement authentic?
  - Am I affected?
  - Do I have to react? If yes, how fast?
  - What are my options?

Issuer and Distributor Requirements

- issuer requirements
  - existing processes can be carried on
  - minimal extra effort and/or technical requirement
- Distributor requirements
  - Presentation according to local formatting style
  - Easy parsing/ability to process

Features

- CAIF has a set of standard sections also present in most of the formats currently in use
  - structurize announcements in a standardized way
  - increase readability
- It provides a set of categories with pre-defined values to increase comparability

Features

- CAIF allows multi-lingual documents
- multiple target groups of readers can be defined reflecting the reader's
  - technical background: admin vs. user
  - organizational overview: employee vs. executive
  - environment: 3rd party software within a suite

Features

- multiple constituencies can be defined
  - constituency dependent assessments
  - markup for constituency dependent text
- CAIF allows to address multiple problems within one document (e.g.“cumulative patch announcements“)

Terminology: Types of Announcements

- CAIF announcement types:

urgency

- alert
- warning
- advisory
- informational
- other

level

- brief
- full
- digest
- other

flavor

- vulnerability-description
- patch-notification
- heads-up
- other

Markup

- CAIF provides a variety of markup elements, to allow for good readability and structuring of the text parts:
  - emphasis: minor, normal and major
  - special strings:vendor, code, program, service, sys-feat
  - files: text, log, config, source, program, lib, binary, path
  - terminal interaction: user input, system

Markup

- elements for text structuring:
  - paragraphs
  - tables
  - lists
  - internal and external links

Text Containers

- `<body>` provides the internal reference to
  - a target group
- `<rlist>` provides the internal references to
  - a target group
  - a problem-id
- The elements contain the text within the main sections

Standard Sections

- Identification *
- revision history *
- subject string *
- summary *
- constituencies
- target groups
- affected systems

- problem ids
  - Attack-vector
  - Attack-requirements
  - Attack-signature
  - Impact
  - exploit status
  - Assessments (see next slide)

* = mandatory element

Standard Sections

- Assessments
  - technical risk
  - probability of occurrence
  - threat
- mitigation
- detailed description
- context information
- solutions
- bibliography
- credits and disclaimer
- rendered copy
- other documents

CAIF - Users

- implemented into services:
  - RUS-CERT, Stuttgart University
  - CERT-VW, Volkswagen AG
- currently introducing the format:
  - dCERT, Deutsche Telekom AG
  - ComCERT, Commerzbank AG

CAIF – interested Users

- talks – interested parties
  - SAP-CERT, SAP AG
  - GNSec GmbH
  - and others

Thank You

Project Home Page:

http://cert.uni-stuttgart.de/projects/caif/

- The presentation at the end of this session is about a possible extension to CAIF
- Questions will be answered and technical details explained at the BOF tonight