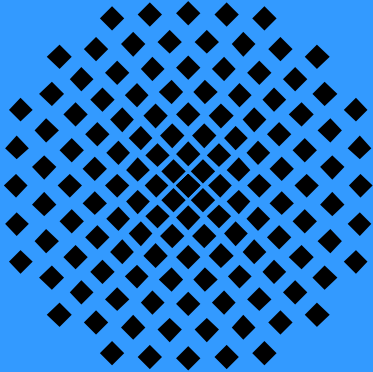
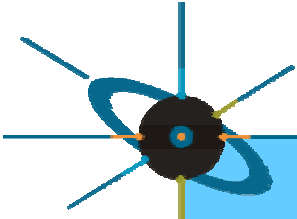


**RUS  CERT**

**[HTTP://CERT.UNI-STUTTGART.DE/](http://cert.uni-stuttgart.de/)**

**OLIVER GÖBEL**



# RUS-CERT

## Rechenzentrum Universität Stuttgart CERT

- founded in 1998
- provides CSIRT-services to Stuttgart University and affiliated organizations
- runs a public advisory service
- does R&D

## SERVICES

- **requests/clearing house**
- **security consulting**
- **incident response**
- **forensic analysis**
  - documentation for internal and public use
  - documentation for prosecution of incident
- **critter analysis**

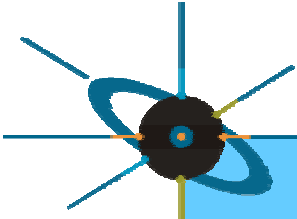
## SERVICES

- **security audit by request**
- **technology watch**
- **vulnerability analysis, validation, announcement**  
⇒ **advisory as the prerequisite for**
- **vulnerability response**  
**security audit triggered by vulnerability response**



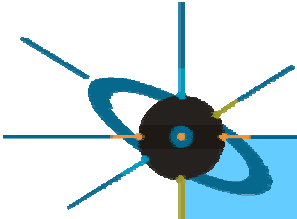
## RESEARCH & DEVELOPMENT

- **software development**
  - **incident handling system**
  - **advisory authoring system implementing CAIF**
- **efforts to integrate these systems**
- **efforts in standardization of advisories: CAIF**



## ADVISORIES

- **running a full scale advisory service is consuming a lot of man-power**
- **advisory issuing organizations focus on the needs of their customers**
  - omission of parts of the problem space
- **advisory issuing organizations use their own format**



## CURRENT SITUATION

- **myriads of different advisory formats**
- **advisories are difficult to compare**
  - different structure**
  - different terminology**
  - different precision**
- **dealing with advisories from different sources requires a lot of time, expertise, and experience**

## CURRENT PROCESS

- **unstructured vulnerability description from security researcher**
  - **optional: CERT/CC advisory**
  - **optional: vendor advisory/patch announcement**
  - **optional: advisory/announcement from other CERT**
  - **optional: other information**
- ⇒ resources are used to produce an advisory**



## CURRENT PROCESS: FLAWS

- **massive multiplication of work**  
comparison, (re-)validation, description
- **reusing other advisories is bound to unclear terms**  
What is commercial use?  
What about automatic redistribution?
- **repeated rewriting tends to introduce errors**  
Different terminology looks like additional information.

# CAIF

## Common Advisory Interchange Format

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

- interchange format for advisories
- automatic redistribution is possible
- format is presentation-independent

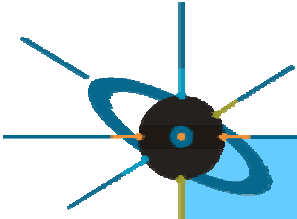
Distributors present advisories in a format familiar to their clients/according their policy.

## CAIF: MAIN GOALS

- **easy usage of advisories issued by others**
- **easy comparison by using meta-information**  
e. g. CVE numbers
- **specializing on fractions of the problem space does no longer hamper effectiveness**
- **co-operation is made easier**  
⇒ **better access to security-related information**

## CAIF: SCOPE OF PROJECT

- **current phase: requirements document**
- **format specification (is being written currently)**
- **author's guidelines**
- **reader's guidelines**
- **category model (draft is finished)**
- **not yet in scope: usage of CAIF in a process - such could be defined in a different project**

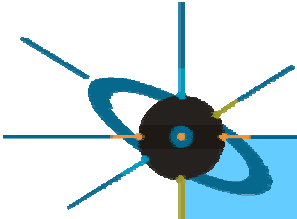


## CAIF REQUIREMENTS

- The following parties exist in a typical process.  
issuers  
(re-)distributors  
readers
- The parties do have different requirements in the process

## ISSUER REQUIREMENTS

- existing processes can be carried on
- minimal extra effort and/or technical requirements
- will possibly conflict with distributor requirements (easy parsing, mechanical processing etc.)



## DISTRIBUTOR REQUIREMENTS

- **presentation according to local formatting style**
- **easy parsing/ability to process advisories mechanically**



## READER REQUIREMENTS

Typically, readers need answers to the following questions:

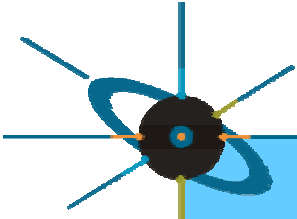
- Is the advisory authentic?
- Am I affected?
- Do I have to react? If yes, how fast?
- What are my options?





## ADVISORY STRUCTURE

- **multiple sections**
- **sections with meta-information**  
both strict syntax and free-form text  
e.g. an issuer-ID and an advisory-ID, reference to the source, contact information
- **sections with free-form text, e.g. description**
- **container collects related documents in CAIF format**



# ADVISORY EXAMPLE

## AS RENDERED BY RUS-CERT

**[platform/product or protocol] Here Goes the Subject**

Source: <http://www.example.com/this/is/the/URL/to/the/main/source.html>

Issuing date

AdvisoryID including an IssuerID

Version

**This is the abstract, giving a brief description of the problem**

### **Affected Systems**

- System 1
- System 2

**Not affected systems** (optional)

- System 3
- System 4

### **Attack Vector**

a brief description of the prerequisites to attack successfully, e. g. *specialty crafted RPC-Request*

### **Impact**

a brief description of the impact. Standardized impact descriptions should be used here,

e. g. *remote host compromise*

### **Vulnerability class**

e. g. *buffer overflow bug*

# ADVISORY EXAMPLE CONT.

## **Severity**

a standardized severity rating related to the impact

## **Context** (optional)

a description of the product or platform affected. This section is useful if rather exotic systems are affected

## **Description**

a description of the problem and its impact

## **Vendor Status** (optional)

The vendor status can also be included in the following section

## **Determination of Vulnerability**

How can the vulnerability of a certain system be determined?

## **Solution** (if applicable)

Usually this section is used to provide references to patches

## **Workaround**

If no solution exists or if a workaround is very likely to be more efficient in most installations a workaround is applicable. This could be a description on how to shut down an affected daemon or similar.

## **Vulnerability ID**

CVE-number, vendor-specific ProblemID (e. g. like Cisco uses them)

## **More Information on this issue**

a list of references to related non-CAIF documents

## **Related Documents**

Container with related CAIF documents



## CRUCIAL META-INFORMATION

- **issuer**
- **document identification**
- **vulnerability identification**  
e. g. by CVE number
- **version**
- **standardized severity rating**

## TEXT MARKUP

- **high level markup**
- **special purpose markup**
  - log file excerpts**
  - terminal interaction**

## CATEGORIES

- **category model based on functional dependency model from relational calculus**
- **categories for:**
  - affected product, vendor name, platform, network service, attack vector, impact, severity, vulnerability class
- **a central category database could provide consistency**
  - Q: How to distribute database updates with CAIF documents?

# SECURITY

- **advisories shall be digitally signed**
- **redistribution shall leave original signatures intact**
- **a rendered copy of the original issue including a signature shall be included in redistributions**



## SYNTACTIC IMPLEMENTATION

- XML DTD
- XML is hopefully human-readable  
compare HTML and MathML
- reference implementation for text and HTML  
rendering is currently operated by RUS-CERT



## FUTURE WORK

- **issue of the yet missing documents**
- **CAIF is intended to be a RfC Draft**
- **develop reference implementation into a distributed system**
  - central database to manage locking and multiple databases**