



EISPP Common Advisory Format Description: Value Lists

Identifier: EISPP-D3-001b-TR

Version 2.0
Date 2004/05/20

IST-2001-35200	EISPP Common Advisory Format Description: Value Lists	EISPP-D3-001b-TR Version 2.0 Date 2004/05/20
----------------	---	--

Table of Content

GLOSSARY 3

1. EXECUTIVE SUMMARY 4

2. LISTS OF STANDARD VALUES 5

 2.1. EISPP Issuers.....5

 2.2. Issuer and RefNum field in "reference" structure5

IST-2001-35200	EISPP Common Advisory Format Description: Value Lists	EISPP-D3-001b-TR Version 2.0 Date 2004/05/20
----------------	---	--

Glossary

BNF	Bacchus Naur Form
CERT	Computer Emergency Response Team
DoS	Denial Of Service
DTD	Document Type Description
EISPP	European Information Security Promotion Program
HTML	Hypertext Markup Language
IDMEF	Intrusion Detection Message Exchange Format
IODEF	Incident Object Description and Exchange Format
PCC	Project Coordination Committee
SME	Small and Medium Enterprise
TBC	To Be Completed
TBD	To Be Defined
URL	Uniform resource location
WP	Workpackage
XML	eXtended Markup Language

IST-2001-35200	EISPP Common Advisory Format Description: Value Lists	EISPP-D3-001b-TR Version 2.0 Date 2004/05/20
----------------	---	--

1. EXECUTIVE SUMMARY

The European Information Security Promotion Programme (**EISPP**) strives to set up a network of expertise with the aim of providing European SMEs with those IT Security services that give them the necessary trust in e-commerce to develop their businesses in that direction. EISPP is a project fund by the EU through the fifth European Framework Program within the thematic program Information Society Technologies (IST). Further information about EISPP can be found at its website, <http://www.eispp.org/>.

Probably the most important security service SMEs have to be provided with, is an advisory service, i.e., the distribution of so-called security advisories that provides system administrators with precise and timely information about new vulnerabilities and what can be done against them. Such information is absolutely essential for IT security, because new vulnerabilities are discovered on a daily basis. IT systems can only be kept secure, if they are regularly upgraded or patched such that the latest security holes are closed again.

One of the corner stones of the EISPP approach towards supplying SMEs with security advisories is a common advisory format, which will enable an easy exchange of advisory data between the four CERTs participating in EISPP. This common format is described in a report with title "EISPP Common Advisory Format Description", which is available from EISPP's website <http://www.eispp.org>. The format is defined using XML, so the various standards and standard tools of the XML-family can be used for advisory processing.

The present document contains those parts of the standard that are subject to more frequent change (or, rather, growth), namely lists of standard values that are to be used within a standard EISPP advisory. The prime example for such a list are standard identifiers for important sources of advisories, e.g., "CERT" for the CERT Coordination Center's advisories, "CERT-VN" for CERT/CC's vulnerability notes, or "REDHAT" for vendor advisories from RedHat, just to name a few.

Once a proper forum for maintaining the EISPP format after the finish of the EISPP project has been established (e.g., as an initiative within TF-CSIRT), this document is likely to be superseded by an actively maintained list.

IST-2001-35200	EISPP Common Advisory Format Description: Value Lists	EISPP-D3-001b-TR Version 2.0 Date 2004/05/20
----------------	---	--

2. LISTS OF STANDARD VALUES

2.1. EISPP Issuers

The "Issuer" field of the identification data in the EISPP advisory format holds an identifier for the (EISPP) CERT that issued the advisory. For FIRST members, the identifier should coincide with the short-name of the advisory as given in the FIRST member information (<http://www.first.org/team-info/>). Currently, the following CERTs are known to issue advisories in the EISPP format:

CERT	Identifier	Country	Contact
Cert-IST	Cert-IST	France	see http://www.first.org/team-info/
esCERT	esCERT-UPC	Spain	see http://www.first.org/team-info/
SESiC Cert	SESiC	Sweden	email sesic@callineb.se
Siemens CERT	Siemens-CERT	Germany	see http://www.first.org/team-info/

2.2. Issuer and RefNum field in "reference" structure

Within the "reference" structure, i.e., the structure used to describe references to resources such as patches, standard vulnerability identifiers, advisories, etc., the EISPP Common Advisory Format Description defines the fields <issuer> and <ref_num>:

<reference>	::= [ref_type] [ref_name] [issuer] [ref_num] [ref_title] <uri>*
<ref_type>	::= code_fix (patch software_upgrade)? advisory [vendor]? technical_information vuln_id other
<ref_name>	::= <i>identifier of this reference local to the present advisory, which may be used to refer to this reference from a formatted-text field via an html <a>-tag.</i>
<issuer>	::= <i>identifier of the issuer of the resource pointed to by the reference</i>
<ref_num>	::= <i>reference number associated with the resource pointed to by the reference</i>
(...)	

The following table lists standardized identifiers for the issuer/source of resources, where column

- "Name" gives the name of the resource.
- "Identifier" gives the standard identifier.
- "Type" gives the type of resource.
- "Ref.Num. Format" gives an example of a valid reference number for the given resource, from which the general format of valid reference numbers can be derived
- "Link" is checked, if the URI of a resource can automatically be determined from standard identifier and reference number. Unfortunately, not all issuers have web sites on which a resource can be found using the resource's reference number.

IST-2001-35200	EISPP Common Advisory Format Description: Value Lists	EISPP-D3-001b-TR Version 2.0 Date 2004/05/20
----------------	---	--

Name	Identifier	Type	Ref.Num. Format	Link?
AusCERT Security Bulletin	AUSCERT	advisory	ESB-2003.0099	X
Bugtraq ID (Security Focus)	BID	vuln.id.	2002	X
Bugtraq mailing list (Posting)	BUGTRAQ	other	312047	X
CERT/CC Advisory	CERT	advisory	CA-2003-04	X
CERT/CC Vulnerability Note	CERT-VN	vuln.id.	484891	X
CIAC Bulletin	CIAC	advisory	N-045	X
CISCO Bug ID	CISCOBUG	vuln.id.	CSCdz29041	
CISCO Security Advisory	CISCO	advisory	cisco-sa-20030221	X
Compaq Security Advisory	COMPAQ	advisory	???	
CVE Number	CVE	vuln.id.	CAN-2002-0230	X
Debian Security Advisory	DEBIAN	advisory	DSA-251	X
EEye Advisory/Alert	EEYE	advisory	AD20021216	X
FreeBSD Security Advisory	FREEBSD	advisory	SA-00:01	X
HP Security Advisory	HP	advisory	???	
ISS Alert/Advisory	ISS	advisory	21824	X
Lotus Notes Technical Note	LOTUS-TN	vuln.id.	???	
Mandrake Security Advisory	MANDRAKE	advisory	MDKSA-2003:016	X
Microsoft Knowledgebase Entry	MSKB	advisory	213541	X
Microsoft Security Bulletin	MS	advisory	MS03-005	X
NetBSD Security Advisory	NETBSD	advisory	1998-001	X
NTBugtraq mailing list (Posting)	NTBUGTRAQ	other	???	
OpenBSD Security Advisory	OPENBSD	advisory	???	
RedHat Security Advisory	REDHAT	advisory	RHSA-2003:029	X
SCO Security Advisory	CALDERA	advisory	CSSA-2003-003.0	
SGI Security Advisory	SGI	advisory	20030201-01-P	X
Sun Alert Notification	SUNALERT	advisory	49475	X
Sun Bug ID	SUNBUG	vuln.id.	???	
Sun Security Bulletin	SUN	advisory	#00220	X
SuSE Linux Security Announcement	SUSE	advisory	SuSE-SA:2003:003	
X-Force Vulnerability Database	XF	vuln.id.	9347	X

Also the identifiers for EISPP issuers as described in Section 2.1 constitute valid identifiers.

IST-2001-35200	EISPP Common Advisory Format Description: Value Lists	EISPP-D3-001b-TR Version 2.0 Date 2004/05/20
----------------	---	--

Document management information

<i>Title</i>	EISPP Common Advisory Format Description: Value Lists
<i>Identifier</i>	EISPP-D3-001b-TR
<i>Confidentiality</i> ¹	PU
<i>Status</i>	A (Approved)
<i>Creation Date</i>	2002/03/19
<i>Version</i>	2
<i>Revision</i>	0
<i>Revision Date</i>	2004/05/20
<i>Deliverable Reference</i>	
<i>Authors</i>	Bernd Grobauer
<i>Keywords</i>	EISPP, XML, Advisory, Format, Exchange

¹ Confidentiality indicator according to the following table

PU	Public
PP	Restricted to other programme participants (including the Commission Services)
RE	Restricted to a group specified by the consortium (including the Commission Services)
CO	Confidential, only for members of the consortium (including the Commission Services)

IST-2001-35200	EISPP Common Advisory Format Description: Value Lists	EISPP-D3-001b-TR Version 2.0 Date 2004/05/20
----------------	---	--

Document History

<i>Version</i>	<i>Date</i>	<i>Reason for modification</i>
0.1	2002-03-19	Document creation (bg)
1.0	2002-03-28	Peer-review in WP3 closed
2.0	2004-05-20	Carried over changes from EISPP version 2.0