

***Vulnerability and Exploit
Description and Exchange Format
(VEDEF)
TF-CSIRT Progress Update***

Ian Bryant
(*VEDEF WG Co-Chair*)

26th May 2006

TF-CSIRT – May 2006: VEDEF WG Update

- Summary of Situation
- Activity Since Last Meeting
- Discussion

VEDEF WG Update

- ▶ **Summary of Situation**
 - Activity Since Last Meeting
 - Discussion

VEDEF – The Background

- Many TF-CSIRT members are engaged in the receipt, processing and dissemination of Vulnerability and Exploit information for their communities
- TF-CSIRT previously helped create IODEF when a similar congruence was found for Incident information
- Vulnerability and Exploit Description and Exchange Format (VEDEF) Working Group established to consider issues

VEDEF – The Environment (1)

- Problem not the lack of data formats, but rather the proliferation of competing and generally incompatible proposals for such formats
- The *de facto* standard for storage of Vulnerability information is Mitre's Common Vulnerabilities and Exposures (CVE)
- **Mitre** agree their OVAL (Open Vulnerability Assessment Language) format is not aimed at VEDEF question
- There are (at least) 8 initiatives for Vulnerability data exchange formats
 - UK Government work on Information Assurance (IA) data exchange formats has identified need for 11 XML families

VEDEF – The Environment (2)

- **TF-CSIRT member activity: EISPP**
 - Initially funded by EU (FP5), with XML Common Format for Vulnerability Advisories now evolved as DAF (Deutsches Advisory Format)
 - In active use with 7 European CSIRTs
- **TF-CSIRT member activity: CAIF**
 - Common Advisory Information Format
 - Initially from RUS-CERT (University of Stuttgart)
 - In active use with 3 European CSIRTs
- **TF-CSIRT member activity: ITDF**
 - Information Triage and Dissemination Format
 - Beta trials completed (*ITsafe* and *WARP/FWA*)
 - XML Schema based on lessons learned produced
 - In active use within UK Government and partners

VEDEF – History of Outreach

- **FIRST**

- Budapest, June 2004 :
BOF broadly supportive
- Singapore, June 2005 :
Little support for idea of BOF

- **IETF**

- Interim INCH meeting, Budapest, June 2004 :
Broadly supportive
- INCH @ IETF60, San Diego, August 2004 :
Little support

- **W3C**

- Informal discussions during 4Q2005, little support

VEDEF – Related Activity (1)

- Trouble Ticketing
 - RT
 - TF-CSIRT members have worked to customise RT to cover Incident Response concerns as RTIR
 - Option has been proposed of similar extension for Vulnerability and Exploit Remediation
 - OTRS
 - Open source Ticket Request System
 - GNU Public License (GPL) with MySQL backend
 - SIRIOS
 - System for Incident Response in Operational Security
 - Extension to OTRS funded in 2003 by CERT-Bund, the German governmental CERT

VEDEF – Related Activity (2)

- Remediation
 - Cisco Proposal
 - Additional XML tags detailing the solution, which customer side software can parse and, optionally, verify devices and download appropriate fixed code
- ICT Description
 - Common Model of System Information (CMSI) proof of concept from same grouping as EISPP
 - Similar needs from UK Government (ICT-NS) and US's XCCDF-P
- Vulnerability Scoring
 - Common Vulnerability Scoring System (CVSS) was US initiative
 - Now under FIRST custody

VEDEF WG Update

- Summary of Situation
- ▶ **Activity Since Last Meeting**
- Discussion

VEDEF – Subgroup Meeting

- April 2006, München DE
 - Hosted by Siemens CERT
- Attendees
 - CERT Verbund members
 - Bayern-CERT
 - DFN CERT
 - RUS-CERT
 - Siemens CERT
 - UK Government
 - CSIA
 - NISCC

VEDEF – Core Format Status

- Attendees at meeting use 3 formats:
 - CAIF (v2.0 under development, open for participation)
 - DAF
 - ITDF
- Consensus
 - No obvious convergence path between the formats
 - No pressing business need to converge
- Options for TF-CSIRT WG
 - Maintain a mapping between these formats
 - Publish the common subset that would be useful to receive from Vendors
 - Possible avenue for ENISA involvement

VEDEF – ICT Description Status

- CMSI format relatively fully evolved
 - Will need to monitor XCCDF-P
- Pressing need to start populating the dataset
 - ICT Descriptions are inherently evolutionary, so significant ongoing maintenance required
 - CSIA / NISCC have good links to US efforts in this area (Mitre and NIST)
- Possible major role for re-purposed TF-CSIRT WG

VEDEF – Trouble Ticketing Status

- Consensus that is useful for Trouble Ticketing systems to explicitly support Flaw Remediation
- Preference for encouraging adoption of such support within Open Source community
 - RTIR
 - SIRIOS
- Possible role of TF-CSIRT WG to agreed common subset of information that would be useful to be supported by Trouble Ticketing systems

VEDEF – Vulnerability Scoring Status

- Initial version of Common Vulnerability Scoring System (CVSS) felt to have limitations
 - Major concern is of Perception, with Base Score being regarded as “THE ANSWER”, ignoring need for localisation
 - Also some practical details
- Now that under FIRST custodianship, interested TF-CSIRT members should seek to get involved with CVSS
 - Worst Case would for it to emerge as a *de facto* Standard which is deprecated by European CSIRTs

VEDEF WG Update

- Summary of Situation
- Activity Since Last Meeting
- **Discussion**

VEDEF – Discussion

- Areas to be considered :
 - Core Format(s)
 - ICT Description Extension(s)
 - Remediation Extension(s)
 - Trouble Ticketing Interface(s)
 - Vulnerability Scoring
- Decisions needed:
 - Future and Composition of Working Group
 - Possible activities at FIRST Annual Conference
 - ICT Description BOF
 - Input into “CVSS 2.x”

Contact Details

***IA Metadata Team
Capability Development Group***

Central Sponsor for Information Assurance (CSIA)

Cabinet Office

6th Floor Stockley House

130 Wilton Road

London

SW1V 1LQ

England

Telephone: +44-87-0114-4561; Ian Bryant
+44-87-0114-4546; Dave Freeman

Facsimile : +44-20-7276-5096

Internet

ian.bryant@csia.gov.uk or david.freeman@csia.gov.uk

<http://www.secdef.org>