draft-debeaupuis-saf-00.txt   T. Debeaupuis
INTERNET DRAFT   HSC
Expires: 19 November 1999   19 May 1999

Security Advisory Format

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

This is first drafty Internet-draft of the Security Advisory Format. A lot of work still to be done in clarifying, removing mistakes and work on the specification of unique names for components impacted by vulnerabilities. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress".

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

To learn the current status of any Internet-Draft, please check the 3id-abstracts.txt listing contained in the Internet-Drafts Shadow Directories on ftp.is.co.za (Africa), nic.nordu.net (Europe), ftp.isi.edu (US West Coast), or munnari.oz.au (Pacific Rim), ds.internic.net (US East Coast).

Distribution of this document is unlimited.

The key words 'MUST', 'MUST NOT', 'REQUIRED', 'SHALL', 'SHALL NOT', 'SHOULD', 'SHOULD NOT', 'RECOMMENDED', 'MAY', and 'OPTIONAL' in this document are to be interpreted as described in RFC 2119 [RFC2119].

Abstract

This memo describes a format for security advisories. An advisory is a document describing a vulnerability of a program, an operating system or, more generally, a software or hardware component of the information system.

This specification tries to minimize changes in issuer and readers current practices (messages style), and by trying to help a program

re-read the advisory tries also to keep advisories easily and friendly readable by humans. It focuses on structure of documents.

This specification is primarily useful for advisories issuers such as CSIRTs [RFC2350] and users and is linked with intrusion detection.

Copyright Notice

1. Table of Contents

2. Changes since last version

Not applicable at this time.

3. Introduction

We face different information issuers :

- CSIRTs
- Vendors
- Groups of people studying vulnerabilities

Different needs :

- Advisory submitters will find in this format a more efficient way to inform the or their community. Internally to the Advisory submit¡ter organisation, this format can also be used to ease the handling of advisories.

- IT security officers : within organizations, IT security officers need to know know what are the vulnerabilities of a specific operating system or software, and in a more general way, a software or hardware component.

- Numerous categories of people (intrusion detection people, researchers, vendors, security consulting firms) are commonly working on advisories as a building block of their work : investigations, auditing softwares (on system or network). A common format will help them entering datas in the databases without spending time to re-organized and formalized advisories. This format aim will also be useful for management tools (IDS frameworks, network security management) to correlate alarms and advisories.

The problem that we are facing today is a lake of standardization between the different formats used to report vulnerabilities.

4. Design goals

The design goals of SAF are as follows :

(1) SAF must suit to security advisory issuers as of users of those advisories,

(2) SAF must be parsable by a program,

(3) SAF should not modify too much current practices and ways of working. SAF should not modify too much advisories looks-and-feel.

(4) SAF must not impose content or order of informations in advisories.

5. Security Advisory Format

5.1. Definitions

Advisory :

A text document announcing to a community a vulnerability in a component of an information system. For example, a software application, a packaging of an application, an operating system, a router hardware.

Vulnerability :

An intrinsic or external provocted fail of a component of the information system leading to decrease the security protection level of a resource.

Impact :

the damage provoked if the vulnerability is exploited.

Patch :

a peace of software replacing the misfunctioning parts of the component to eradicate the vulnerability.

Workaround :

a procedure describing a change in the configuration that can protect the component from being corrupted by a the exploit of a vulnerability without applying patches.

5.2. Advisory encoding

SAF is a token based labeling language. A SAF advisory is a 7 bit US-ASCII document or 8 bit ISO 8859-1 text document. Implementations MUST support both encodings.

5.3. Sections

Advisories are composed of sections. Sections order is NOT enforced.

5.4. SAF grammar

A SAF document can be encoded intro two formats : an XML document conforming the DTD provided in this document, or a readable and parsable text format (to be defined).

```
<!-- ================================================= -->
<!-- This is the XML Security Advisory Format DTD      -->
<!--                                                   -->
<!-- Author: Tristan Debeaupuis                        -->
<!-- ================================================= -->
<!-- $Id:$


                                                       -->
<!-- ================================================= -->
<!-- Entities
<!entity % isoent system>
%isoent;

<!-- ================================================= -->
<!-- Elements                                          -->

<!element advisory - -
```

```
           (advisory ( head, body? ) >

   <!attlist advisory
           opts cdata "null">

   <!element head - o (title, ref?, author, abstract?)

   <!element title - o
        #pcdata>

   <!element author - o (name, thanks?,
                          (and, name, thanks?)*)>
   <!element name - o (#pcdata) +(newline)>
   <!element and - o empty>
   <!element thanks - o (#pcdata)>
   <!element date - o (#pcdata) >
   <!element ref - - (#pcdata) >

   <!element abstract - o (#pcdata)>

   <!element body - o (#pcdata)>

   <!-- The original source of this advisory (my organization name) -->
   <!element source - - (#pcdata) >

   <!-- Title of the advisory, usually the subject of the mail -->
   <!element title - - (#pcdata) >

   <!-- Date of issue of this advisory. If it is an update, the current date --
>
   <!element date - - (#pcdata) >

   <!-- A free text describing the problem -->
   <!element description - - (#pcdata) >

   <!-- Language used in this advisory -->
   <!element lang - - (#pcdata) >

   <!-- Level of impact -->
   <!element impact - - (#pcdata) >
   <!attlist impact
        level cdata "dos|admin"> <! Dos : Deny of Service -->
   <! This list (dos, admin) must be expanded in future versions of -->
   <! this document -->

   <!-- List of impacted components -->
   <!element objects - - (object)+>

   <!-- Free text describing the vulnerability on this component -->
```

```
   <!element object - - (#pcdata) >

   <! Objects name must be defined uniquely among all the    -->
   <! advisories. So, a central repository with fast update  -->
   <! will probably be necessary.                            -->
   <! This name will be the same used in the IDEF (Intrusion -->
   <! Detection Exchange Format)
   <!attlist object
           name cdata #required
           impacted cdata "yes|no|unknown|maybe"
        patchref cdata "null">

   <!-- Reference to the exploit script or URL to an exploit -->
   <!-- May be used with caution - URL can change            -->
   <!element exploit - - (#pcdata) >

   <!-- A free text describing a way to stop the problem -->
   <!element workaround - - (#pcdata) >

   <!-- List of patches -->
   <!element patchs - - (#pcdata) >

   <!-- The filename of this advisory -->
   <!element filename - - (#pcdata) >

   <!-- ================================================= -->
   <!-- end of ADVISORY DTD
   <!--
        Local Variables:
        mode: sgml
        End:                                              -->
   <!-- ================================================= -->
```

6. Security Considerations

This document describes a format which aim is not to improve security of advisories (transmission, trust, archiving). It can help security officers having a better view of the vulnerabilities impacts on their systems by facilitating advisories re-treatment by automatic or semi-automatic programs.

7. References

[RFC2234] "Augmented BNF for Syntax Specifications: ABNF", D. Crocker, P. Overall, RFC 2234, November 1997.

[RFC2350] "Expectations for Computer Security Incident Response" N. Brownlee, E. Guttman, RFC 2234, June 1998.

[RFC2119] Key works for use in RFCs to Indicate Requirement Levels, S. Bradner, RFC 2119, March 1997.

[US-ASCII] United States of America Standards Institute (now American National Standards Institute), X3.4, 1968, "USA Code for Information Interchange". ANSI X3.4-1968 has been replaced by newer versions with slight modifications, but the 1968 version remains definitive for the Internet.

8. APPENDIX 1 - Current advisories semantics

Note : the annexes are only for information. They are helpful and will be deleted in the future because we are not trying to standardize CSIRTs current formats, but to propose an evolution and a merge of those formats.

This section uses ABNF but is not a lexical definition of advisories but rather a semantical grammar description of advisories.

CERT

Types of advisories :
- Vendor initiated bulletins

```
<CERT-VB> =     <HEADING> <INTRODUCTION>
               <FORWARDED-TEXT>
               <HOW-TO-CONTACT>
               <CERTCC-INFORMATIONS>
```

- CERT advisories

```
<CERT-BULLETIN>     =    <HEADING> <INTRODUCTION>
               <DESCRIPTION>
               <IMPACT>
               <SOLUTION>
               <APPENDIX>*
               <NO-WARRANTY>
               <HOW-TO-CONTACT>
               <CERTCC-INFORMATIONS>
               <COPYRIGHT>
```

```
    <APPENDIX> =         1*<VENDOR-INFORMATION>

    <VENDOR-INFORMATION> =   <VENDOR-NAME>
                   <CURRENT-STATE>
```

- Advisories released by other CSIRTs and forwarded by CERT with or without added-value.
- CERT Summaries

CIAC

- CIAC Bulletin

```
    <CIAC-BULLETIN> =   <HEADING> <SUMUP> <DESCRIPTION>
                   <VENDOR-SPECIFIC-INFORMATION>*

    <HEADING>  =        <LOGO> crlf <TYPEOFBULLETIN> crlf crlf <TITLE> crlf
                   crlf <DATE><ADVISORY-NUMBER>

    <SUMUP>    =        <HRULE> crlf <PROBLEM> crlf <PLATFORM> crlf <DAMAGE>
                   crlf <SOLUTION> crlf <HRULE> <VULNERABILITY> crlf
                   <ASSESSMENT>

    <DESCRIPTION> =

    <VENDOR-SPECIFIC-INFORMATION> =
```

AUSCERT

```
   <AUSCERT-ADVISORY>  =    <TITLE-BANNER> crlf
                  <SUMMARY> crlf
                  <CONTENT>

   <TITLE-BANNER> =    <PARTNUM>
                  <TITLE>
                  <DATE>
                  <LAST-REVISED>
                  <INTRODUCTION>

   <LAST-REVISED> =    <DATE> " " <ACTION>

   <CONTENT>      =    <DESCRIPTION>
                  <IMPACT>
                  <WORKAROUND>
                  <MOREINFO>
                  <THANKS>
                  <WARRANTY>
                  <ADDRESS>
                  <REVISION-HISTORY>
```

MICROSOFT

- Paragraphs are left aligned, close to the border
- Lists are indented at 1 and 3 spaces
- Sections are introduced by a section name without number, underlined with "=".
  A blank line is used before a section title and the section text is directly
  added on the line following the section underlines.
- Tokens are :

Originally Posted : date of first release of the advisory,

Summary : sum-up. What is affected, on which systems, what's the impact, is there are patches, workarounds ?

Issue : What's the technical problem of the vulnerability ?

Affected Software Versions : list of affected components

What Microsoft is Doing : tell if patches (fixes), knowledge base article are available, tell the fix references for each impacted components.

What customers should do : explanation of fixes (supported but not regression tested). No specific information.

More Information : references (URLs) for this advisory, and the Knowledge Base article.

Obtaining Support on this Issue : Reference to subscribe to support.

Acknowledgements : thanks to people who has reported the problem.

Revisions : list of revision of this document. For each revision, date of revision and comment are given.

```
      <MICROSOFT-BULLETIN> =   <TITLE>
                     <POSTED-DATE>
                     <REVISED-DATE>
                     <SUMMARY>
                     <ISSUE>
                     <AFFECTED-SOFTWARE>
                     <WHAT-MICROSOFT-DOING>
                     <WHAT-TO-DO>
                     <WORKAROUND>
                     <MORE-INFORMATION>
                     <REVISIONS>
                     <WARRANTY>
                     <COPYRIGHT>
                     <MAILING-LIST-INFO>
```

CISCO

```
   <CISCO-SECURITY-NOTICE>  =    <FIELD-NOTICE> <HRULE>
                       <REVISION>
                       <RELEASE-DATE>
                       <CONFIDENTIALITY>
                       <SUMMARY>
                       <AFFECTED-TEXT>
                       <IMPACT>
                       <BUGREF>
                       <LIST-OF-AFFECTED-AND-PATCHES>
                       <WORKAROUND>
                       <EXPLOITATION>
                       <NOTICE-STATUS>
                       <DISTRIBUTION-REFERENCES>
                       <REVISION-HISTORY>
                       <CISCO-SECURITY-PROCEDURES>
                       <HRULE>
                       <COPYRIGHT>

   <SGI-ADVISORY> =         <HEADINGS>
                       <WARNING>
                       <DESCRIPTION>
                       <IMPACT>
                       <WORKAROUND>?
                       <SOLUTION>
                       <ACKNOWLEDGMENTS>
                       <SGI-CONTACTS>
   <HEADINGS>     =         <TITLE>
                       <NUMBER>
                       <DATE>

   <SOLUTION>     =         <PATCH-URL>
                       1*(<OS-NAME>   <VULNERABLE>   <PATCH-NUMBER>
                       <ACTION>)

   L0pht

   <L0PHT-ADVISORY> =       <HEADINGS>
                       <DESCRIPTION>
                       <IMPACT>
                       <SOLUTION>

   <HEADINGS>     =         <URL-REF>
                       <RELEASE-DATE>
                       <COMPONENT-IMPACTED>
                       <OPERATING-SYSTEM>
                       <IMPACT>
                       <PATCH-AVAILABILITY>

    - Repent Security Incorporated, RSI

    <RSI-ADVISORY> =         <TITLE>

    <TITLE>        =         <PART-NUM>
                        <BANNER>

    - Herv  Schauer Consultants, HSC

    <HSC-ADVISORY> =         "(" <SOURCE> ") " <TITLE> "(" <DATE> ")" crlf
                        <OBJETS-TOUCHES>
                        <IMPACT>
                        <DESCRIPTION>
                        <PARADE>
                        <CORRECTIFS>

    <OBJETS-TOUCHES> =       *<OBJET-TOUCHE>

    <CORRECTIFS>   =
```

Acknowledgements

Many thanks to Barbara Fraser and Jean-Michel Cornu for there support.

Author's Address

Tristan Debeaupuis
Herv Schauer Consultants
142, rue de Rivoli
75001 Paris
France

Phone: +33 141 409 700

Email: Tristan.Debeaupuis@hsc.fr

Comments should be sent directly to the author.