Security bulletin publication at AusCERT using "EzESB"

by Matthew Braid and Robert Lowe

Abstract

This paper examines a problem – the publication of large volumes of security bulletins via various media (such as web and email). It then goes on to discuss the requirements of a tool which may be used to automate much of this manual work. Finally, the development, current features and future enhancement of the tool (EzESB) used by AusCERT for this purpose, will be discussed.

The objective of this paper is to give other members of FIRST insight into the development and use of this tool and more details about how AusCERT publishes bulletins. Other FIRST members may be offering similar services or may have a future requirement for such a service. We hope that this paper will stimulate discussion between teams with an interest in the publication of security bulletins.

The paper does not go into any real technical depth. Anyone who disseminates (a large number of) security bulletins would probably be interested in this paper. Analysts and software engineers developing tools for the publication of security advisories may find AusCERT's solution to this particular problem interesting. Managers directly involved in the work flow of such teams or team members may also find this paper of interest.

Introduction

AusCERT (the Australian Computer Emergency Response Team, Australia's National CERT) is funded primarily by member subscriptions. Members vary in size and include commercial, government and educational organisations. Accurate and timely notification of security threats and vulnerabilities is a key service provided by AusCERT to members. According to a 2003 survey of current AusCERT members, 68% of members rated AusCERT's security bulletin publication as "essential" and 32% as "useful" - the most valuable service provided by AusCERT.

AusCERT writes and publishes Advisories, Updates and Alerts which all contain original content. AusCERT also publish (with permission) selected External Security Bulletins (ESBs) from vendors and security researchers. In 2003, AusCERT published 872 ESBs and 827 in 2004. In addition to external advisory content, AusCERT prefixes each ESB with consistent header fields. This gives

recipients a concise summary of the bulletin, including the affected platforms and the severity of the threat or vulnerability.

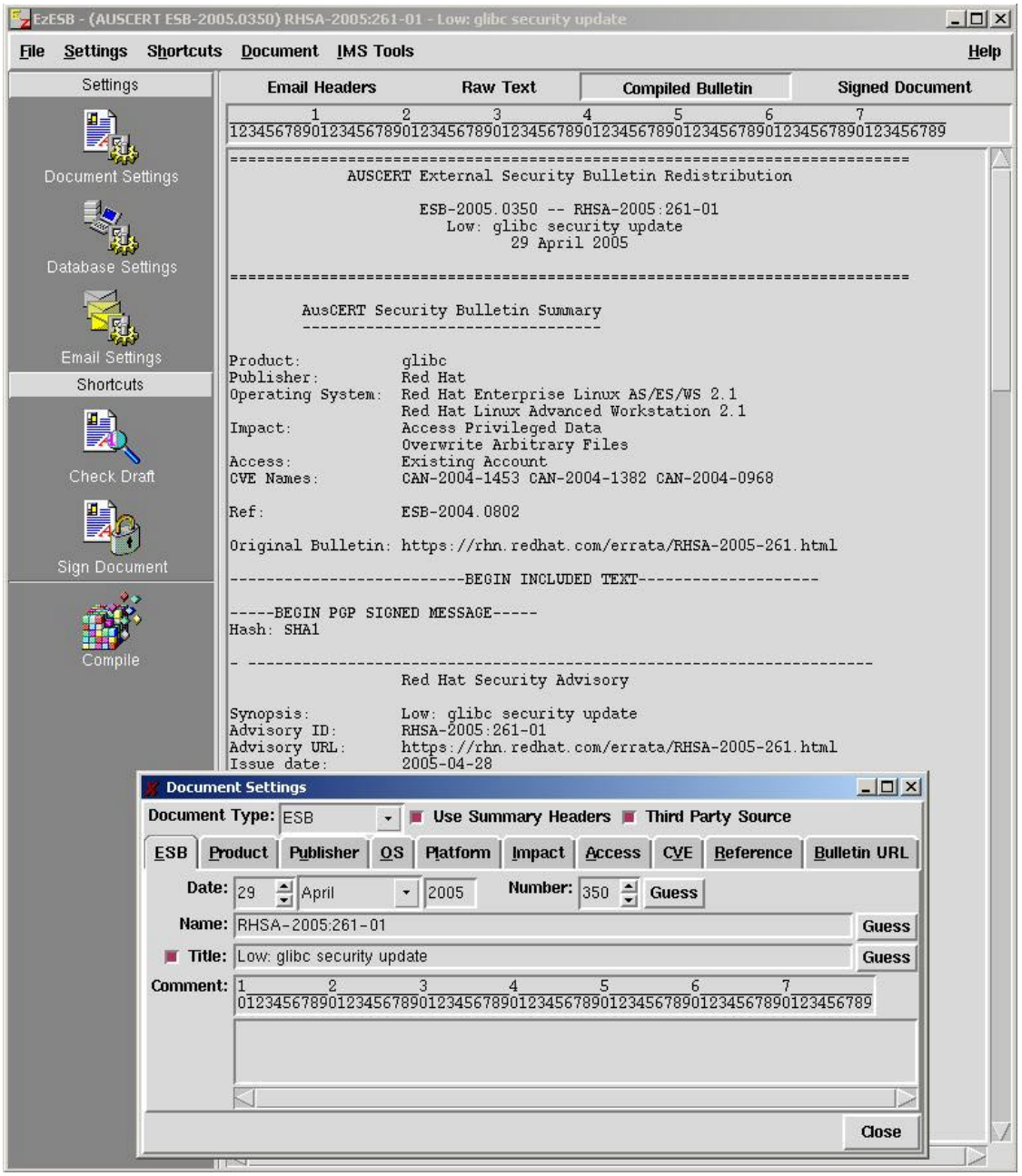
The Requirements

Initially, every bulletin was edited manually - a labor intensive process, prone to inconsistencies. All AusCERT bulletins are published via email to subscribers and posted on the website. More recently, a summary of important bulletins is sent to subscribers by mobile phone SMS, as part of the early warning service offered by AusCERT. Peer review of advisories by other coordination centre staff is a critical part of maintaining the consistent level of quality and accuracy of AusCERT bulletins which is expected by members. And finally, many vendor bulletins adhere to a consistent format, allowing for the certain summary fields to be deduced automatically.

In response to these requirements "EzESB" (Easy ESB) was developed. It was initially developed in an ad-hoc manner by one of the coordination centre staff because he was tired of the tedious nature of ESB publication. However, it has grown to be identified as a key application used by the AusCERT coordination centre.

The Tool

EzESB was programmed in Perl. It utilises the Perl-Tk graphics library to create an X Windows GUI and stores data in MySQL databases. These implementation decisions were made because of the integration with various other applications/data sources, a requirement for rapid application development and existing Perl programming skills in-house. AusCERT runs EzESB on a centralised UNIX sever and while the code should be portable to other flavours of UNIX or Linux, several strong dependencies and the level of integration would make this non-trivial.



EzESB features include:

- The ability to create a bulletin from a file or create a new bulletin from scratch.
- Integration with the AusCERT email client (exmh) to enable users to easily start creating an ESB from an incoming email message.
- PGP signature verification of the incoming bulletin using GnuPG and a shared public key ring.

- The ability to strip the email headers from the bulletin to be distributed, but still retaining them for reference, if required. It is also possible to strip all but the PGP signed portion of the bulletin.
- Automatic deduction of the key AusCERT summary headings from Apple, CIAC, Cisco, Debian, EEye, FreeBSD, HP, iDEFENSE, ISS, MacroMedia, Microsoft, Red Hat, SGI, Sun, UNIRAS and US-CERT advisories.
- Automatic generation of a unique identifier for each type of bulletin.
- Compiles the header information into a complete bulletin, but this header information may still be edited.
- Integration with standard UNIX spell checking.
- The ability to save bulletins for later editing and the ability retrieve previously saved bulletins from a database.
- Sending of draft bulletins for peer review by email. These show not only the content of the bulletin, but other configuration values which will influence the resulting publication (e.g. if a summary is also to be sent via SMS, or not).
- Signing of the outgoing bulletin, using GnuPG.
- Email and/or publish the signed bulletin to the AusCERT website.
- Supporting profile based bulletin distribution, by allowing subscribers to choose to receive only bulletins of certain types by setting their profile preferences via the AusCERT web site.
- SMS a summary notification of selected important bulletins to an SMS list.

Of these features, there is a high degree of integration with other applications and data sources, both standard (GnuPG, SMTP, MySQL, ISpell and Exmh) and AusCERT internal systems (Web content management, Mobile phone SMS and the Incident Management System).

Future Enhancements

Whilst this tool saves significant amounts of time of AusCERT analysts, AusCERT is committed to the future improvement and development of EzESB. In line with this goal, the following future enhancements are planned:

- Further refinement of automated processing. The ability to deduce more information from a wider variety of external security bulletins.
- Integration with AusCERT's mailing list application, enabling targeted bulletins to specific (possibly encrypted) mailing lists.
- Improvement for the handling of updates and revisions of bulletins.
- A structured revision history of bulletins.
- Migration of all AusCERT public communications to EzESB, e.g. scheduled maintenance and reduced service announcements as well as "the week in review" weekly email.

- Templates for AusCERT authored publications (alerts, advisories and updates).
- The ability to efficiently publish multiple external bulletins in a single AusCERT ESB.
- Automatic “time out” of member-only advisories to be viewable by the public after a predefined period.

Conclusion

EzESB has saved significant amounts of staff time within the coordination centre. In a recent server migration, EzESB was considered an essential tool for AusCERT staff. Some may not consider this tool in the realm of Incident Response, per se. However, we believe that its ability to effectively publish analysed and trusted information consistently to Administrators and Security professionals may be of interest to members of the FIRST community. The distribution of security related bulletins may be a requirement or goal of other FIRST members. If so, we would welcome further discussion of this activity and the tools used to perform it.

Contact

AusCERT is situated in Brisbane, Australia (GMT+10) and can be contacted through the following means:

Email: auscert@auscert.org.au

Web: http://www.auscert.org.au

Telephone: +61 7 3365 4417

Facsimile: +61 7 3365 7031

Postal: AusCERT
The University of Queensland
Brisbane QLD 4072
Australia