

## REQUEST TRACKER INCIDENT RESPONSE (RTIR) SOFTWARE TO BE UPGRADED AND EXPANDED

TERENA and Best Practical Solutions, LLC have signed a contract for a project to upgrade and expand the RTIR (Request Tracker for Incident Response) software package. The project started on 6 October 2005 and will run for a period of 18 months. The cost of the project, estimated at 95,350 US dollars, will be carried jointly by nine Computer Security Incident Response Teams (CSIRTs) in Europe.

Nine CSIRTs in Europe are involved in the project:

- \* ACOnet-CERT, a team of Vienna University Computer Center (Austria);
- \* CERT POLSKA, a team of the NASK Research and Academic Computer Network research and development organisation (Poland);
- \* CERT.PT, a team of the Fundação para a Computação Científica Nacional (Portugal);
- \* GOVCERT.NL, a team of Stichting ICTU (the Netherlands);
- \* IRIS CERT, a team of Entidad Pública Empresarial Red.es (Spain);
- \* JANET-CERT, a team of the JNT Association trading as UKERNA (United Kingdom);
- \* LITNET CERT, a team of Kaunas University of Technology, Information; Technology Development Institute (Lithuania);
- \* SUNet CERT, a team of the Swedish Research Council (Sweden);
- \* SWITCH-CERT, a team of the Swiss Academic and Research Network foundation SWITCH (Switzerland).

The RTIR software is a useful tool supporting CSIRTs in their daily work, registering incidents and keeping track of the workflow in handling the incident. RTIR is open-source software, making it possible for interested technical specialists to upgrade the tool and to expand it with additional features. JANET-CERT, the CSIRT of the British national research and education network organisation UKERNA, has been one of the earliest users of RTIR in Europe, and has contributed to the further development of RTIR using the services of Best Practical Solutions, LLC, original creators of the software.

As more CSIRTs in Europe have adopted RTIR as their incident handling tool, TERENA's task force TF-CSIRT has established an RTIR working group, which will have the current application extended, making it more stable and will have functionality added, thus making it more adaptable for general use by both new and established CSIRTs.

TF-CSIRT is a group of Computer Emergency Response Teams who meet to forward and champion network and computer security across Europe under the umbrella of TERENA. The RTIR-WG is a working group within TF-CSIRT, which coordinates the development of new features for RTIR.

In March 2005, the RTIR Working Group completed a Requirements Document, describing the specifications of the planned extension of the software. Negotiations with Best Practical Solutions have led to agreement about the terms of a contract for carrying out this work. The report was prepared by Andrew Bone of JANET-CERT and Carlos Fuentes Bermejo of IRIS CERT.

The Requirements Document summarises the expectations of the upgraded system.

- \* it will carry out routine actions automatically;
- \* it will support team functionality by automatically presenting appropriate information;
- \* it will enable CSIRT's to meet an increasing workload without possible expansion to the team;
- \* it will speed up the current application;
- \* it will incorporate encryption/decryption of messages;
- \* it will support more active gathering of information from CSIRT's networks, communities and from relevant external sources as required.

CSIRT teams have contributed their own experiences and comments when dealing with local Incidents and their present workflow (recognising that there are both areas of similarity and areas of difference) with regards RTIR. The Working Group has also examined other products and local systems in formulating the requirements.

The Working Group has used the following assumptions and conventions, most of which apply to system design but some have bearing on requirements:

- \* the core of the software will be a database;
- \* incident handling activities are centred on correspondence (predominantly originated as e-mail) consisting of messages known as Incident Reports (IR's).
- \* replies to IR's will be needed and these will be known as Investigations;
- \* sequences of exchanges with a single correspondent about a single topic are important entities and should be stored within one Incident;
- \* when an action results in a restriction of service it will be recorded as a Block.
- \* An incident is an event of significance in security coordination and information for management and will encompass one or more IR's, Investigations and blocks;
- \* The governing aims of incident handling activities is a prompt and accurate response to all information received, and to reply to outstanding correspondence as soon as practicable, or as dictated by a local Service Level Agreement (SLA).

The products of the project work will be delivered in three batches, in April and October 2006 and in April 2007. These deliverables will be accepted subject to a positive review by a committee of technical experts from the CSIRTs concerned, which will be chaired by Robert Morgan of JANET-CERT.

Each milestone build of RTIR will be a full, supported release intended for production deployment. As part of this project, Best Practical will provide instructions and support for migration to each milestone build. Each milestone build will be delivered via TERENA to the RTIR Working Group of TERENA's task force TF-CSIRT for acceptance testing and feedback.

More information about the project to upgrade and extend the RTIR software can be obtained from the TERENA Secretariat: [news@terena.nl](mailto:news@terena.nl)

More information about TF-CSIRT can be found at:

<http://www.terena.nl/tech/task-forces/tf-csirt/>

ckg/05/10/05



**TRANS-EUROPEAN RESEARCH AND EDUCATION NETWORKING ASSOCIATION**  
For more information, please contact the TERENA Secretariat  
Tel: +31(0) 20 530 4488, email: [news@terena.nl](mailto:news@terena.nl)

<http://www.terena.nl>