Message from Dave Kelsey sent to the GDB in July 2005.

Dear all,

As you already know...

We have created a group working on Security Vulnerabilities. This started as a GridPP activity and has grown to include EGEE and LCG. This has been presented at the EGEE Middleware Security Group, at EGEE-03 in Athens, at the JRA1 All Hands in Brno and at GridPP13 in Durham. We have received general support for the approach, and a number of people have joined the activity and several bugs have already been registered. Work is just starting to assign these.

The policy of the group is stated below. We are seeking approval by EGEE PEB, LCG PEB and GridPP PMB to ensure that we have the full support of the project management and that all questions of liability and responsibility are fully understood and accepted. We are also expecting strong support in getting high priority security problems fixed quickly. The success of the group will be measured by their success (or lack of it!) in improving the quality from the security point of view.

Why is it necessary to ask for management approval?

A significant number of site sys-admins feel strongly that the policy by which the group is operating is flawed. Their preferred model is to follow the standard CERT/CC approach of "responsible disclosure". This approach is that the group contacts developers to get fixes produced. During this time they tell no-one of the existence of the problem. After a timeout (typically 45 days), CERT goes fully public, whether or not the problem is fixed. This has the advantage of applying strong pressure to developers to produce timely fixes and keeping information private during the 45 days.

Our approach is different. Because we are an ***internal*** group (CERT is external to all developments) we are in a different position. We cannot go public (we see this as the responsibility of JRA1/SA1 management) and moreover we feel that in certain circumstances we may need to inform our registered sites before the 45 days has been reached (on a closed mail list).

Given that we (the group) will never inform external customers of our middleware and distributions, it is important that JRA1 and SA1 and any other developers and distributors realise that we are expecting them to take on this responsibility. There is also a risk from informing site sys-admins before a fix is available as info may leak out.

We also feel that as the middleware matures the handling of security vulnerabilities should move to the CERT/CC approach of full "responsible disclosure"

Please can this be discussed by both the EGEE and LCG PEBs. We ask for approval of the group's policy below. I will also submit to the GridPP PMB for their approval.

Many thanks,
Regards,

Dave Kelsey

Security Vulnerability Group

We have formed a security vulnerability group, internal to EGEE, LCG, and GridPP. The purpose of this is to inform developers and deployment people of vulnerabilities as they are identified and encourage them to produce fixes or to reduce their impact.

A subset of the vulnerability group is a core group currently led by Linda Cornwall from RAL. This core group manages the group including its membership. Sysadmins and Developers in EGEE, LCG and GridPP are entitled to join the group, others at the discretion of the core group.

Information on vulnerabilities will be entered in a database which is readable only by members of the group.

If urgent action is needed then system administrators at registered sites will be informed (OSCT is responsible for defining the mechanism to do this).

Mirror entries will be entered into the world-readable JRA1 savannah database but with the details missing.

The vulnerability will be assigned to the appropriate development cluster and a target time for resolution (usually 45 days) will be assigned.

If a solution isn't available by the target time sites will be informed of the problem by forwarding information on the specific vulnerability and a risk assessment to the appropriate list(s) defined by OSCT.

The vulnerability group will not publish information on vulnerabilities to which there isn't a solution, however once the sites receive this information we cannot guarantee they will not publicise it.

We will also produce a web page accessible to anyone with an appropriate grid certificate listing the number of vulnerabilities and their status for each piece of software, to enable progress to be tracked and encourage the resolution of problems.

We will report progress including the number of vulnerability bugs that are open for each piece of software, including those that are open beyond their target time, to JRA1 and SA1 management on at least a monthly basis.

The work is carried out on a best efforts basis. We are a group facilitating the tracking and reduction of potential vulnerabilities, including providing a process where potential problems can be kept private pending their resolution.

JRA1 and SA1 management are responsible for the software and deployment along with their own policy on the public release of vulnerability information.

All liability or responsibility, if any, to sites and/or other customers, internal or external, of the grid software rests with the project(s) as a whole and its management and not with the vulnerability group.

We encourage open source middleware developers to work towards the adoption of open responsible public disclosure of all security vulnerabilities after a suitable period of time. This responsibility remains with JRA1 and SA1 management and not with the vulnerability group.

Notes :-

Any vulnerability that has been exploited is considered an incident and should not be handled by the vulnerability group, but be handled by agreed incident response procedures. The vulnerability group aims to reduce the likelihood of incidents.

We are not doing security operations, the OSCT (EGEE SA1 Operational Security Coordination Team) will define the appropriate mailing list or contacts for informing sites and system administrators.

The process for handling the vulnerabilities will be reviewed as we progress.