Operational Security Coordination Team

DRAFT work in progress.

This topic contains guidance and notes for the OSCT on handling security advisories and incidents.

Incidents Reported on the Security CSIRTS list (project-lcg-security-csirts@in2p3NOSPAMPLEASE.fr)

Incidents should be handled according to the agreed incident handling process. The OSCT-DC has responsibilities defined here.

Advisories Received from the Grid Security Vulnerability Group (GSVG)

Please note that the GSVG process leading to public disclosure and the target-date time windows have not yet been officially approved by the project.

Advisories which have been assessed by the GSVG Risk Assessment Team (GSVG-RAT) will be sent to the OSCT at project-lcg-security-support@cernNOSPAMPLEASE.ch.

GSVG-RAT classifies each vulnerability according to a scale of risk as LOW, MEDIUM, HIGH and EXTREMELY CRITICAL (further details of the classification scheme are available on the GSVG site).

Not all GSVG advisories will be sent to the OSCT. The OSCT receives advisories where either action to mitigate the vulnerability at Grid sites is anticipated or a known vulnerability will not be patched before it reaches its *target date*. Also, if the GSVG is notified of vulnerabilities which are **already public** then the OSCT is notified immediately of the result of the assessment.

For LOW, MEDIUM and HIGH vulnerabilities a completed vulnerability advisory will be available. In view of the urgency, notification of an EXTREMELY CRITICAL vulnerability is likely to be less complete. The process of the two cases are documented separately below

GSVG severity EXTREMELY CRITICAL vulnerability advisory handling by OSCT

On receipt of an EXTREMELY CRITICAL advisory the following responsibles and/or deputies should be contacted immediately either by email or a follow-up telephone call to attend a telephone conference call _contact details to be provided_-

- ♦ Ian Bird - Head of LCG/EGEE Operations (SA1)
  ♦ Maite Barroso Lopez - Manager Operations
  ♦ Nicholas Thackrey - Deputy Manager Operations
  ♦ Markus Schulz - Manager Certification and Testing (SA3)
  ♦ Laurence Field - Deputy Manager Certification and Testing
  ♦ Claudio Grandi - Manager gLite Middleware development
  ♦ John White - Deputy Manager gLite Middleware development
  ♦ Ake Edlund - Head of Security EGEE
  ♦ Dave Kelsey - Deputy Head of Security EGEE, Chair JSPG
  ♦ Mingchao Ma - Deputy LCG/EGEE Security Officer
  ♦ Romain Wartel - LCG/EGEE Security Officer, OSCT Chair
  ♦ ROC Security Contacts and ROC Managers
  ♦ relevant contacts from the GSVG should also be contacted to be available for advice.

The meeting will decide on an appropriate course of action including the assignment of responsibilities for -

- co-ordination actions
- content of advisories to be distributed
- mitigation measures

GSVG severity LOW, MEDIUM and HIGH vulnerability advisory handling by OSCT

GSVG advisories will contain:

- a description of the vulnerability
- the severity assigned by GSVG-RAT
- a unique identifier for tracking
- the so-called *target date*, which is the date the GSVG makes the advisory fully public on its website and mailing lists
- (optionally) advice on fix or mitigating action that can be taken
- (optionally) additional relevant information

The length of the time-window between the GSVG issuing an advisory and the *target date* depends on the severity of the vulnerability according to an agreed scale.

The GSVG-RAT can be contacted for clarification by mail at
project-egee2-gsvg-rat@cernNOSPAMPLEASE.ch

In each case, the OSCT, by email or other discussion, must decide on a course of action which may include:

- Immediate _heads up_ notice to sites. This would be appropriate in cases where the severity of an issue or the lack of an immediate patch requires that site administrators must be informed to decide on local mitigating action such as restricting or shutting down a grid service. The *heads up* is designed to act as a warning and give the site administrators the information they need to make an informed decision on local action including a projected timescale for further action.

- Issue an Operations Advisory notice to sites. In cases where no patch will be made available (such as architectural or design limitations which can only be mitigated by appropriate processes being followed at a site) an appropriate advisory should be issued. Recommended actions such as documentation changes or procedural changes should be forwarded to the responsible parties.

- If and when a patch is available, following build and certification, the normal grid operations release procedure is applied. The GSVG advisory will be included in the release notes at this stage and OSCT may be involved in drafting the content of the notes.

Heads up notices and advisories should be sent as follows -

- ♦ Use the EGEE broadcast tool
  ♦ Select to send to: *Production Site Admin* and *PPS Site Admin*
  ♦ Do **NOT** send to the LCG Rollout
  ♦ Add into CC: project-lcg-security-contacts@cernNOSPAMPLEASE.ch **AND** project-lcg-security-support@cernNOSPAMPLEASE.ch

In case of the EGEE broadcast tool not being available the advisory should be sent to project-lcg-security-contacts@cernNOSPAMPLEASE.ch **AND** project-lcg-security-support@cernNOSPAMPLEASE.ch to include a statement that the site administrators should be contacted locally if necessary.

Template advisories

Example and Template advisory

NREN contacts

NRENs/ROCs mapping

-- Main.ineilson - 25 Oct 2006

This topic: LCG > OSCTProcs
Topic revision: r13 - 2009-07-29 - MingchaoMa