Vulnerability Handling – experience from the October Torque issue

Ian Neilson

CERN

GDB November 8th 2006

The Vulnerability

- Details of and exploit method for a vulnerability in the Torque batch server allowing any user authorized to run jobs the ability to become root.
- The report was dated March 2006 but publicly disclosed in October 2006. The history between discovery and disclosure is not known.
  - http://www.securityfocus.com/archive/1/449248
  - http://csirt.fe.up.pt/docs/TORQUE-audit.pdf

The Basic Timeline

- Thurs 2006-10-19
  - 00:45 Vulnerability disclosed on BugTraq
- Friday 2006-10-20
  - 07:59 Reported to GSVG
  - 12:11 OSCT notified of Extremely Critical risk
  - 15:49 “heads-up” advisory sent to sites
  - 19:58+ Patch advisory(s) released

GSVG notice to OSCT

- After the initial disclosure and report, GSVG members worked on verification and started to test a preliminary patch
- Initial GSVG notice to OSCT -

SUBJECT : Extremely Critical bug in GSVG

A vulnerability in the Torque pbs_mom was reported today to the Grid Security Vulnerability Group, and we think that it may be serious enough to justify an immediate alert to the site security contacts. The essence of the bug is a possible root compromise in pbs_mom of Torque.

The bug is already revealed to publicity on the BugTraq list. Details can be found on:
http://csirt.fe.up.pt/docs/TORQUE-audit.pdf

One quickfix patch is already on its way by Ake Sandgren.

The GSVG assessed the bug as Extremely Critical.

If the root escalation is proven on the grid, and no patch is provided soon, even a global Torque shutdown should be considered.

OSCT ‘heads-up’ to sites

- Since it was Friday and likely to be towards end of the day before the patch could be rolled out it was decided to warn sites -

SUBJECT: [HEADS UP] Torque/OpenPBS local root privilege escalation vulnerability

The Grid Security Vulnerability Group (GSVG) and the Operational Security Coordination Team (OSCT) have been made aware this morning of a security flaw affecting Torque/OpenPBS, which was initially published on BugTraq on Wed, 18 Oct 2006 23:45:

http://csirt.fe.up.pt/docs/TORQUE-audit.pdf

The vulnerability is being handled by GSVG (bug #20883). It has been confirmed and has been rated EXTREMELY CRITICAL.

A patch has been built and in currently being tested and certified.

We expect the patch to be out within the next hours and more details about this security vulnerability will be published before the weekend.

Release Announcement(s) – 1.1

- First announcement made on behalf of OSCT (19:58)

SUBJECT: Torque/OpenPBS local root privilege escalation vulnerability

```
Dear Site Admins and Security Contacts,

As announced earlier on today, Torque is currently affected by a security flaw.
A patch is now out and all affected sites are invited to upgrade immediately.

================================================================================
Torque/OpenPBS local root privilege escalation vulnerability

Grid Software Vulnerability Group Security Advisory

-- Date: 2006-10-20
-- Background
Torque/OpenPBS is the batch job manager that implements the mechanism for job submission to the local
    computing nodes.

Pbs_mom is Torque/OpenPBS's component that manages the lifecycle of batch jobs on the Worker Nodes and
    provides the node status to the Torque/OpenPBS server part.

-- Affected Software
gLite <= 1.5, LCG <= 2.7.x, gLite <= 3.0.x.

-- Affected Components
All versions of OpenPBS and Torque are affected.

For gLite 3.x the affected meta-package are:

    …….
```

(continued)

Release Announcement(s) – 1.2

(continued)
For LCG 2.x the affected meta-package is lcg-WN_torque.

For gLite 1.x the affected component is "Torque Client for the gLite Worker Nodes".

EGEE Grid software installs torque-1.0.1p6 by default, but it is known that sites tend to use newer versions of Torque or older versions of OpenPBS. Such setups are also vulnerable.

-- Vulnerability Details
By creating a malicious symbolic link, a local attacker could easily gain root privileges on any node running pbs_mom (typically Worker Node).

The Torque/OpenPBS's pbs_mom is writing the output and error messages from user jobs to predictable files using root privileges.

Unfortunately, Torque/OpenPBS is affected by a flaw that can enable a malicious user to symlink to any file on the system from these Torque/OpenPBS files, causing the output/error messages to be appended to arbitrary files. As a result, it is possible for the attacker to create, modify or execute arbitrary files on the system with root privileges.

-- Grid Security Vulnerability Group Response The Grid Security Vulnerability Group views this issue as EXTREMELY CRITICAL and strongly recommends that all sites using Torque/OpenPBS upgrade to the latest version of Torque/OpenPBS IMMEDIATELY, following the directions of the "Installation Notes" section.

-- Further documentation
This advisory is also available at the following URL:

http://www.gridpp.ac.uk/gsvg/

-- Installation Notes
The following rpms have been made available;
…..
(continued)

Release Announcement(s) -1.3

(continued)
These are appropriate to fix what is distributed with gLite 3.0 and LCG-2_7_0.

They are available in the appropriate repositories for each distribution.
http://glitesoft.cern.ch/EGEE/gLite/APT/R3.0/rhel30/RPMS.updates/
http://grid-deployment.web.cern.ch/grid-deployment/gis/apt/LCG-2_7_0/sl3/en/i386/RPMS.lcg_sl3.security/

We are distributing the full rpm set, but please note that the vulnerability is patched by upgrading the pbs_mom on the WNs. An upgrade of the head node is not strictly required.

After the upgrade, please ensure that pbs_mom has restarted properly (the rpm update should do this automatically).

-- Credit
This vulnerability was disclosed[1] in the BugTraq mailing list by Luis Miguel Silva (ISPGaya). The vulnerability was reported to the GSVG by Eygene Ryabinkin (RRC-KI).

-- Disclosure Timeline
2006-10-18 Vulnerability disclosed in the BugTraq list by Luis Miguel Silva (ISPGaya).
2006-10-20 Vulnerability reported to GSVG by Eygene Ryabinkin (RRC-KI)
2006-10-20 Initial response from the Grid Security Vulnerability Group
2006-10-20 OSCT notified of the vulnerability
2006-10-20 Initial patch provided by GSVG
2006-10-20 Updated sources available
2006-10-20 Updated LCG and gLite packages available
2006-10-20 Release preparation completed
2006-10-20 Public disclosure
2006-10-20 Site Admins and LCG Security Contacts notified

-- References
1. The original BugTraq thread:
http://www.securityfocus.com/archive/1/449248/30/0/threaded

Release Announcement(s) – 2.1

- Second announcement made by the release team 20:13 (links to first)

SUBJECT EXTREMELY CRITICAL UPDATE for grid sites using Torque

Dear all (or more specifically, administrators of sites using Torque 1)

The Grid Security Vulnerability Group have been notified of a vulnerability which they have assessed and consequently classed as "EXTREMELY CRITICAL".

This vulnerability exists in an external dependency of the gLite middleware and as such would normally require a patch to come from the providers of the external software. However, by good fortune a patch is available within the gLite middleware teams and this patch is now in the repositories of the EGEE production and pre-production services.

To re-iterate; in the normal course of events, external packages are distributed with the gLite middleware for convenience *only*. Distribution of the external packages does *not* imply any responsibility for this external software on the part of the gLite middleware teams. As the gLite middleware teams do not maintain the external packages of the middleware, they will not normally create patches for these external packages. That they are doing so on this occasion is a special, one-off event.

The details of the vulnerability and the update can be found here:

http://glite.web.cern.ch/glite/packages/R3.0/updates.asp

For more detailed information including fixed bugs, updated RPMs, configuration changes and how to deploy, please go to the 'Details' link next to each service on the 'Updates' web page.

Release Announcement(s) – 2.2

All issues found with this update should be reported using GGUS: www.ggus.org

Best regards,
The gLite Middleware Teams

Note on Torque 2
==========
Patched versions of the RPMs for Torque 2 can be found here:
http://hepunx.rl.ac.uk/~traylens/rpms/torque/2.1.3-1cri_sl3_2st/
These are used entirely at the site's own risk.

Process Issues

- Gave the sites the information for them to decide –
  - GSVG risk classification (EC) not well understood
  - Some wanted recommendation/instruction on action in the heads-up
    - Policy not explicit when the heads-up was given
- Release process longer than anticipated
  - Could have overlapped test/certification and repository update
- Confusion as EGEE Broadcast tool failed to work
  - Duplicate messages as different people tried
- Because of delay and the weekend sites began to close down
  - Announced on the roll-out list
- Security Contact lists incomplete
  - Missing ROC-contact roles from the GOCDB
- Concern over support policy for packages in “external” repository
  - Who is responsible?
- Initially GSVG email to OSCT was sent to wrong list (minor)
  - Support and discussion lists