SSC4 au CC-IN2P3

Le message d'alerte

This is about the Security Service Challenge 4 (SSC4) test incident running at your site please read this mail carefully to the end, and take the proper actions.

SSC4 is executed under the supervision of EGI-CSIRT as part of the Security Services Challenge (SSC). More information about the SSC can be found at

    http://cern.ch/osct/ssc.html

Information on the evaluation can be found at

    https://twiki.cern.ch/twiki/bin/view/LCG/SSC4Evaluations

You are asked to follow the normal computer security incident response procedure, but you MUST_NOT take any collective action against the VO of the offending user(s).
In particular the certificates used here have the (SSC4) string in the certificate subject. Please make sure not to operate on other certificates.

-- ALERT --
Consider any network activity in which the following IPs

134.158.170.110 and 195.140.243.2

are involved as malicious.

Please handle this SSC4 incident according to the normal computer security incident response procedure with the two exceptions listed below:

1. No sanctions must be applied against the Virtual Organization (VO)
   that was used to submit the job.
2. All "multi-destination" alerts must be addressed to the e-mail list
   which has been designated for the SSCs:

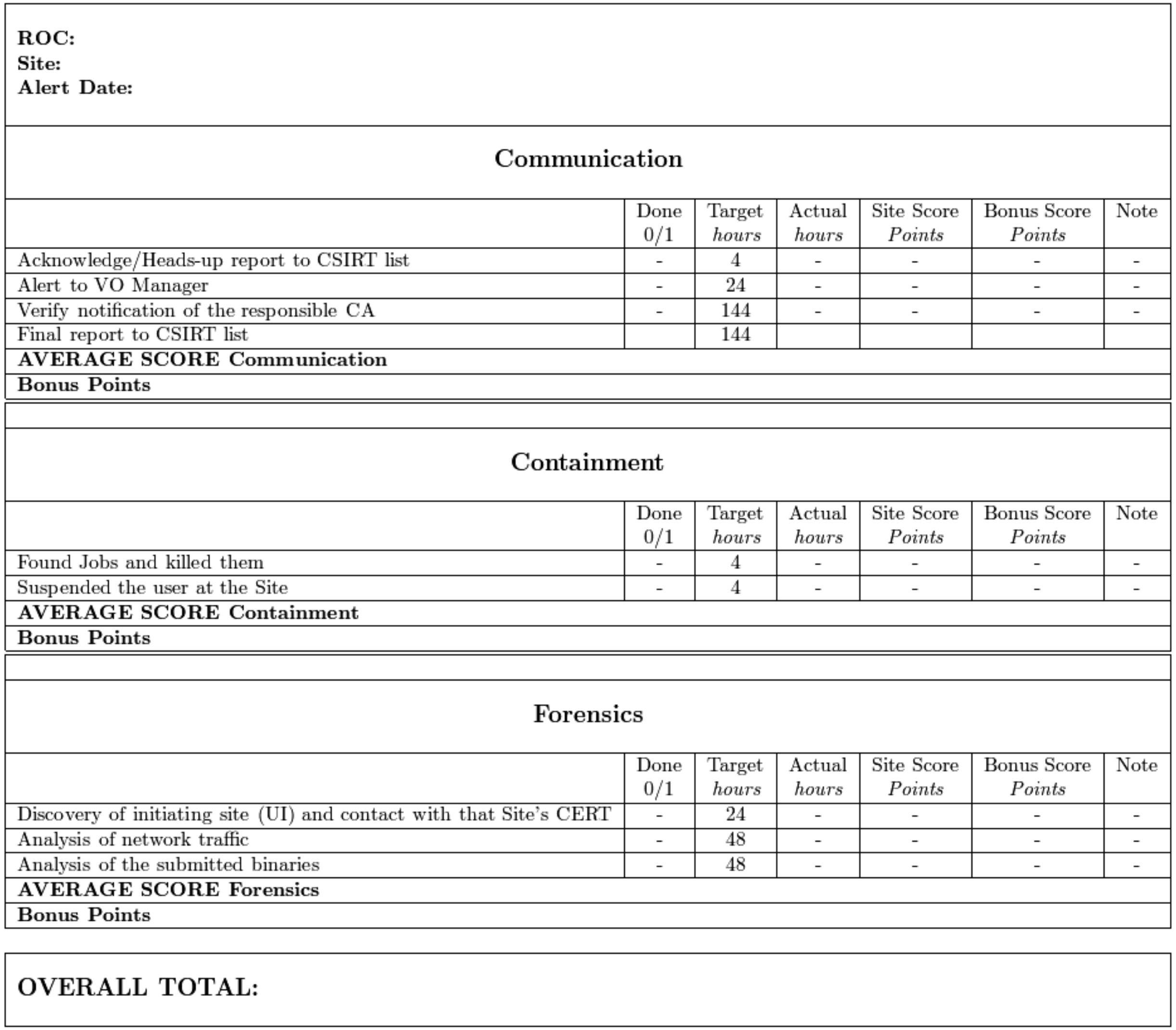
    project-egee-security-challenge@cern.ch

DO NOT use project-lcg-security-csirts@in2p3.fr for Security Challenges.
Instead, insert the originally intended "multi-destination" address(es) in the body of your message.
3. SSC4 also includes one of the experiments Pilot-Job-Frameworks, so be prepared to communicate to more entities in order to gather all needed information to resolve the incident and to minimize the impact of the security activities on the affected VO.
If you communicate to other entities like cern-cert, atlas-VO, atlas-cert, CAs that provided the affected certificates, please always CC

    project-egee-security-challenge@cern.ch

- http://cern.ch/osct/ssc.html
- https://twiki.cern.ch/twiki/bin/view/LCG/SSC4Evaluations

Evaluation Template



ROC:
Site:
Alert Date:

Communication

	Done 0/1	Target *hours*	Actual *hours*	Site Score *Points*	Bonus Score *Points*	Note
Acknowledge/Heads-up report to CSIRT list	-	4	-	-	-	-
Alert to VO Manager	-	24	-	-	-	-
Verify notification of the responsible CA	-	144	-	-	-	-
Final report to CSIRT list		144				
AVERAGE SCORE Communication						
Bonus Points						

Containment

	Done 0/1	Target *hours*	Actual *hours*	Site Score *Points*	Bonus Score *Points*	Note
Found Jobs and killed them	-	4	-	-	-	-
Suspended the user at the Site	-	4	-	-	-	-
AVERAGE SCORE Containment						
Bonus Points						

Forensics

	Done 0/1	Target *hours*	Actual *hours*	Site Score *Points*	Bonus Score *Points*	Note
Discovery of initiating site (UI) and contact with that Site's CERT	-	24	-	-	-	-
Analysis of network traffic	-	48	-	-	-	-
Analysis of the submitted binaries	-	48	-	-	-	-
AVERAGE SCORE Forensics						
Bonus Points						

OVERALL TOTAL:

Final report

Dear CSIRTs,

Here is an update and the final report of the test security incident at IN2P3-CC. This last message should have been posted for a while. I apologize for this very late report.

All times are local time (GMT+2)

**** INCIDENT DESCRIPTION

A suspect activity was reported to us on Thursday May 27th at 13h36 local time by Sven Gabriel <sveng@nikhef.nl>.

Those two IP addresses were involved in a malicious network activity.

- 134.158.170.110 => ccwl0549.in2p3.fr.
- 195.140.243.2 => wunderbar.geenstijl.de.

**** FIRST ANALYSIS

At the time we received this alert, the worker node "ccwl0549.in2p3.fr." (134.158.170.110) was running a suspect job handling a TCP connexion to "wunderbar.geenstijl.de" (195.140.243.2).

This job was a pilot job from the VO Atlas submitted from the UI 128.142.195.138 (voatlas61.cern.ch.) thru our CE 134.158.105.168 (cclcgceli06.in2p3.fr).

The submitter certificate was :

> /C=UK/O=eScience/OU=CLRC/L=RAL/CN=graeme andrew stewart (ssc4)

The final job user certificate was :

> DN=/O=dutchgrid/O=users/O=nikhef/CN=Sander Klous (SSC4)

The first analysis shows up that other jobs have been run before we were alerted, since 2010/05/25 17h05 until 2010/05/27 15h33.

189 pilot jobs with the submitter certificate "/C=UK/O=eScience/OU=CLRC/L=RAL/CN=graeme andrew stewart (ssc4)" were run, and only two user jobs were run with the certificate "DN=/O=dutchgrid/O=users/O=nikhef/CN=Sander Klous (SSC4)".

The network analysis reports network connexions with the malicious IP 195.140.243.2 (wunderbar.geenstijl.de.) on TCP ports 80 and 25443 from two IN2P3-CC worker nodes.

134.158.170.110 => ccwl0549.in2p3.fr. (between 2010/05/25 at 17h15 and 2010/05/26 at 18h58)

134.158.171.28 => ccwl0691.in2p3.fr. (between 2010/05/27 at 12h1O and 2010/05/27 at 15h33)

Consider any connexion with those two IPs as suspect.

Final report

**** ACTIONS

The two certificates have been suspended at our site and the VO managers informed on May 27th 2010.

The suspect job was terminated on 2010/05/27 at 15h33 after data collection and the IP address "195.140.243.2" was filtered. The worker nodes "ccwl0549.in2p3.fr" and "ccwl0691.in2p3.fr" were finally isolated from the production farm.

**** COMMUNICATION

- 2010/05/27 13h36 : Alert from Sven Gabriel <sveng@nikhef.nl>
- 2010/05/27 14h27 : Acknowledge to Sven Gabriel
- 2010/05/27 14h29 : Incident reported to "project-egee-security-challenge@cern.ch"
- 2010/05/27 18h02 : Incident reported to the "atlas" VO managers (acknowledged)

- 2010/05/28 09h21 : Incident reported to "atlas-adc-csirt@cern.ch" - Atlas VO (acknowledged)
- 2010/05/28 09h47 : Malicious activity of 195.140.243.2 reported to "abuse@kixtart.nl" - IP owner (not acknowledged)
- 2010/05/28 09h57 : Incident reported to the DUTCHGRID CA (acknowledged)
- 2010/05/28 10h04 : Incident reported to the eScience CA (acknowledged)
- 2010/05/28 10h14 : Incident reported to CERN in charge of the User Interface IP (acknowledged)

*** SUBMITTED BINARY ANALYSIS

A shell script called "gridssc.sh" has been run on our worker nodes. This script first determines the architecture of the running host, downloads the binary for the relevant OS (in our case "lutra_Linux_64_rh5") from the IP 195.140.243.2 (wunderbar.geenstijl.de.) on TCP port 80 using "wget" (have a look at http://wunderbar.geenstijl.de/lutra/), and finally executes the binary.

The downloaded program "lutra_Linux_64_rh5" searchs for writeable directories on the system, tries to run "crontab" and "at", and reports the results to the same host 195.140.243.2 (wunderbar.geenstijl.de) using the IRC protocol. This IP runs an IRC server using SSL (InspIRCd) on TCP port 25443.

In our case "crontab" and "at" failed because standard users are not allowed to use these services on our worker nodes.

This analysis seems to confirm that not privilege escalation have been gained. In the real life, the two worker nodes involved in the incident should have been fully reinstalled.

Bilan humain

- 5 personnes impliquées dans la gestion de cet incident
  - 2 admins grille
  - 1 admin stockage grille
  - 1 admin réseau
  - 1 coordinateur sécurité