



CVE-2008-0166, lessons learned and actions

David Groep, Nov 7nd, 2008

CVE-2008-0166

National Cyber-Alert System

Vulnerability Summary for CVE-2008-0166

Original release date: 05/13/2008

Last revised: 09/05/2008

Source: US-CERT/NIST

Static Link: <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-0166>

Overview

OpenSSL 0.9.8c-1 up to versions before 0.9.8g-9 on Debian-based operating systems uses a random number generator that generates predictable numbers, which makes it easier for remote attackers to conduct brute force guessing attacks against cryptographic keys.

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 7.8 (HIGH) (AV:N/AC:L/Au:N/C:C/I:N/A:N) (legend)

Impact Subscore: 6.9

Exploitability Subscore: 10.0

CVSS Version 2 Metrics:

Access Vector: Network exploitable

Access Complexity: Low

Authentication: Not required to exploit

Impact Type: Allows unauthorized disclosure of information

Approx time line

- Released: Tue, May 13
 - (CVE number reserved: Jan 15, 2008!)
 - Picked up by Roberto Cecchini same day
- Tue May 13
 - 'informal' request for assessment sent to PMA members
 - several CAs start revoking affected end-entity certs
- Wed May 14
 - Bulk checking tool distributed to the PMA lists
 - PMA itself checked IGTF distribution
 - Affected CA root certs identified and re-generated
- Fri May 16
 - Updates IGTF distribution with updated CA
 - Release coordinated with OSCT EGEE/LCG public advisory
 - Still limited (~50%) CA response on affected EE certs

The week after

- Mon, May 19
 - 31 responses received and appropriate action taken
 - Still 10 CAs did not respond at all
- Tue, May 20
 - Sent 'final' warning to personal addresses
 - End of day: 36 responses received, 4 pending
 - One pleaded extension of checking till Friday ...
- Wed, May 21
 - For those CAs that have a EE list retrievable, did checking myself
 - For selected CAs, bypassed CA and contact Ees
 - Publication of list of keypairs escalates the issue
- Thu, May 22 – ...



What did we learn?

- Requests for action from PMA should be univocal and clear in what action is required
- CA contact addresses are ill-watched
 - And people behind the addresses are not always the same people as those technically operating the CA
 - Response can take *N* mails and still wait for a week
 - Response to **all** mails is even more important than action
- The RPs need an IGTF-wide response
- CA suspension can be done
 - But is very upsetting and must never be done lightly
 - And needs couple of key people to share responsibility
- The PMA structure was not ROBAB proof

Implemented structure and process

- For *public* vulnerabilities only
 - Communicate to relying parties that the PMA is aware
 - Publish this statement on-line and send to the PMA announce list(s) - with URL for updated information
- A IGTF wide Risk Assessment Team assesses issue
 - Jim Basney, Jens Jensen, Willy Weisz, Yoshio Tanaka, Jinny Chien, David Groep, Vinod Rebello (igtf-rat@eugridpma.org)
 - Define expected time for responses from Cas
 - Interacts with RAT and CSIRT teams from RPs

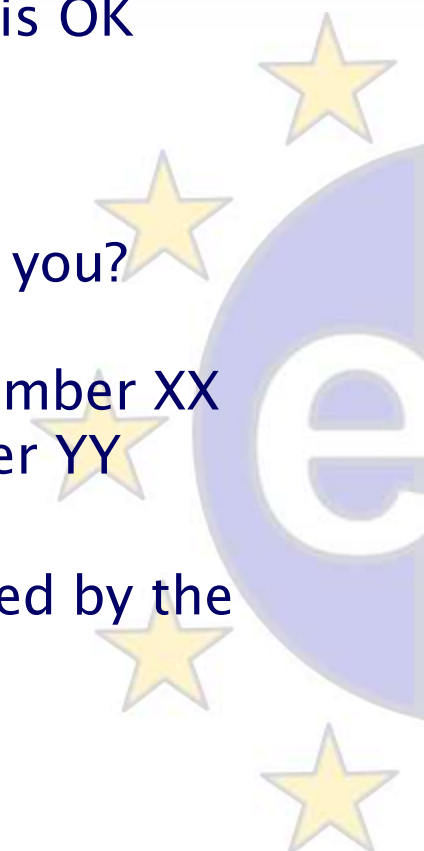


Response

- Send query to all CAs
 - Initial address taken from .info file
 - Signed email, but not encrypted
 - Define expected response
 - For urgent issues, use per-CA escalation procedure
- CA response
 - All Cas are expected to send an ACK next business day
 - Full response before RAT-established dead line
 - CAs can of course ask for extension
but need to keep responding to RAT requests any time!
- Escalation
 - per-PMA core team (for EUGridPMA: DaveK, UrsulaE, Jan Jona J, DavidG) agrees what happens in case of serious malfunction – if rapid action is indeed needed

CA actions requested

- **Respond** to all RAT emails!
 - Check that email address in your meta-data is OK
 - And there is somebody watching
- Deposit your escalation procedure
 - For example: do you want the RAT to phone you?
 - 1: send email to this personal address
 - if no response: 2: call me at the office on number XX
 - if no response: 3: call me at home on number YY
 - if no response: 4: call ZZ at number AA
 - This information is kept private and encrypted by the RAT members (incl. the PMA chairs)
 - And never used otherwise...
- Act within the RAT time line



ROBAB

- PMA operations were too concentrated
 - Shared control passwords to more people
 - For EUGridPMA also AndersW can now do everything
 - web sites hosting machine access
 - domain name management (.org+.info)
 - email forwarding configuration
 - CVS management
 - Enable all chairs to sign the IGTF distribution with the SAME key
 - Securely distributed to MikeH, YoshioT, AndersW
 - Replication of key web sites (already did that for the IGTF distribution itself)



RAT

- See Jim's presentation ...



