
# How the RIPE NCC handled the recent security threats -

## Heartbleed, Shellshock, Poodle

Ivo Dijkhuis

NCC Services WG | RIPE 69 | November 2014

# Recent Security Threats



- CVE-2014-0160
  **Heartbleed** (OpenSSL)

- CVE-2014-6271
  **Shellshock** (Bash)
  (CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187)

- CVE-2014-3566
  **Poodle**(bleed) (SSLv3)

# Vulnerability Mitigation Process (1)



1. Intelligence gathering
   a) public / closed / internal mailing lists
   b) social media
   c) responsible disclosure reports
2. Risk assessment
   a) probability and impact
   b) remotely exploitable / privilege escalation?
   c) external services affected?
      ⇨ immediate mitigation!

# Vulnerability Mitigation Process (2)



3. Mitigate
   a) Test update, change or workaround in test environment
   b) apply software update, configuration change in production ⇨ automated configuration management

4. Test mitigation in production
   a) scanning tools, custom scripts
   b) external services (e.g. SSL Labs)

5. Inform public
   a) www.ripe.net , NCC Announce mailing list

# How does this affect RIPE NCC Services?



- Impact of Heartbleed, Shellshock and Poodle?
  - no evidence of exploitation found
  - additional security measures taken
  - RIPE NCC web services now incompatibility with older software (IE6/XP 2001-2006)

- 2015 Security Activities
  - external security audits of our web services
  - increase DDoS resiliency
  - Increase involvement in Security community

# Questions?