Alerts, Advisories
30 October — 17 December

5 advisories/update sent

- EGI-SVG-2015-7835: Xen host escalation [Critical]
- EGI-SVG-2015-7183: Libnss remote execution [Critical]
- EGI-SVG-2015-9707: Java [Unknown/High] – with Update
- EGI-SVG-2015-3193: OpenSSL [Low/NA]

Critical CVE handling 30 October — 17 December

- Critical vulnerability:
  - CVE-2014-9322 (kernel): 2 new, 1 reappearing
  - CVE-2014-6271/6277 (shellshock): 1 new
  - CVE-2015-3245 (libuser): 1 new, 1 reappearing
  - CVE-2015-718{1,2,3}(libnss): 103 new, 4 reappearing
    → 9 sites suspended
- Security re-Certification (SEC05):
  - 3 site **in progress**: MY-UTM-GRID, MY-UM-SIFIR, RO-03-UPB

Critical CVE handling
CVE-2015-718{1,2,3} Statistics

Communications, ...

Subject **[EGI #9943] Critical Vulnerability Exposed - CVE-2015-7181/2/3 - NGI_NL - NIKHEF-ELPROD**

Reply to csirt@rt.egi.eu

Cc security@biggrid.nl

```
** GREEN information - Community Wide Distribution                    **
** This can be circulated  within  the EGI community                  **
** see https://wiki.egi.eu/wiki/EGI_CSIRT:TLP for distribution restrictions **

Dear security contact for NIKHEF-ELPROD (cc to NGI security officer),

** What EGI-CSIRT expects from you **

- Please acknowledge this message by replying to this mail before 3 December 2015, 12:00 CET

- Follow the instructions to update libnss in
  https://wiki.egi.eu/wiki/SVG:Advisory-SVG-2015-CVE-2015-7183

** Why you received this mail **

Our monitoring indicated a vulnerable version of libnss is installed on the
following node(s) at your site:
```

Critical CVE handling
CVE-2015-718{1,2,3} Suspension

- AsiaPacific INDIACMS-TIFR
- AsiaPacific MY-UPM-BIRUNI-01
- NGI_IL WEIZMANN-LCG2
- NGI_IT CRS4
- NGI_IT INFN-BOLOGNA-T3
- NGI_IT INFN-ROMA2
- NGI_PL IFJ-PAN-BG
- ROC_LA CBPF

Critical CVE handling CVE-2015-718{1,2,3}

- Large campaign, most sites fixed in few days only
- New (internal) tool to automatically create tickets
- Several issues identified within RT-IR:
  - Tickets initially not sent to Requestor!
  - Custom fields (site, NGI, constituency) ignored
  - Proper ACLs currently impossible to deploy

  $\rightarrow$ RT-IR upgrade should be given priority
- 'Lost/Missed' emails: any suggestion?