Scanning CMS

Zuzana Duračinská • zuzana.duracinska@nic.cz •
22.09.2017, Stockholm

CSIRT.CZ

- National CSIRT in Czech republic
- Operated by domain registry .CZ
- Role and duties of National CSIRT are part of national legislation on cyber security
- Operator of National CSIRT have to have **formal agreement** with National Cyber and Information Security Agency

Formal agreement...

...CZ.NIC commits to prevention from cyber attacks by using for example passive detection tools or if needed actively looking for vulnerable or poor configured devices available from the Internet...

How to deal with vulnerable CMS?

- Idea: scan websites in .cz for vulnerable CMS
- Legal analysis was done prior to testing
- Legal analysis were done on Rom-O testing, testing CMS or other similar tests
- 2 separate studies stated that such tests are not illegal under certain circumstances
- Character of the company was taken into account, provision of tests, communication of results...

How to perform such tests?

- Tested subject have to be informed about vulnerabilities that were discovered
- Testing has to be transparent
- Minimum intervention principle should be used
- Obtained information about vulnerabilities should be well safeguarded
- Testing should be communicated into community through established communication channels

How was testing done

- Script ran 3 times
- 1. Full zone was tested
- 2. Only websites running outdated WP or Joomla were retested
- 3. Websites that were informed were re-tested
- We were interested in WP older than 4.7.5 and Joomla older than 3.7

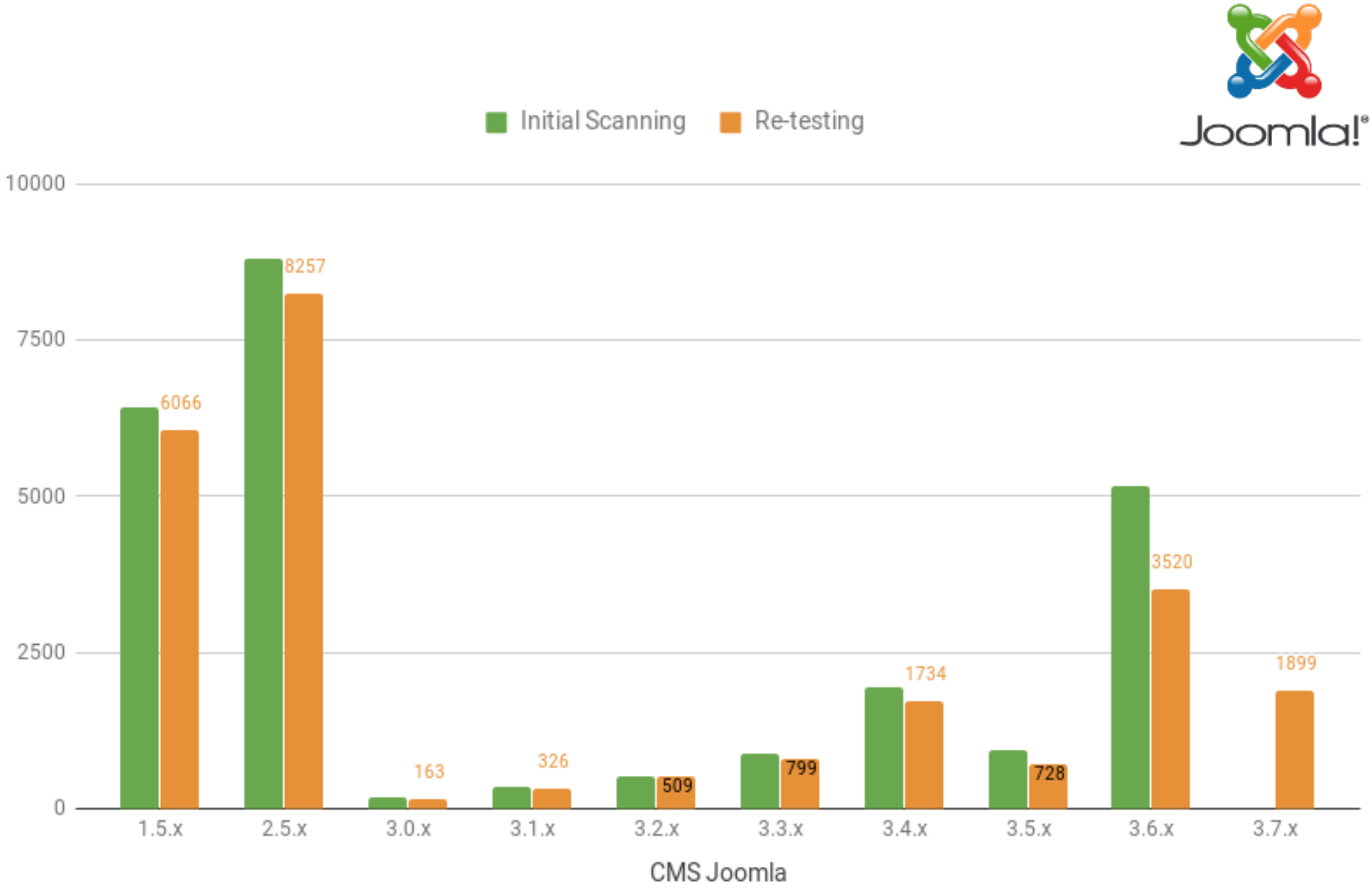
How we gathered information

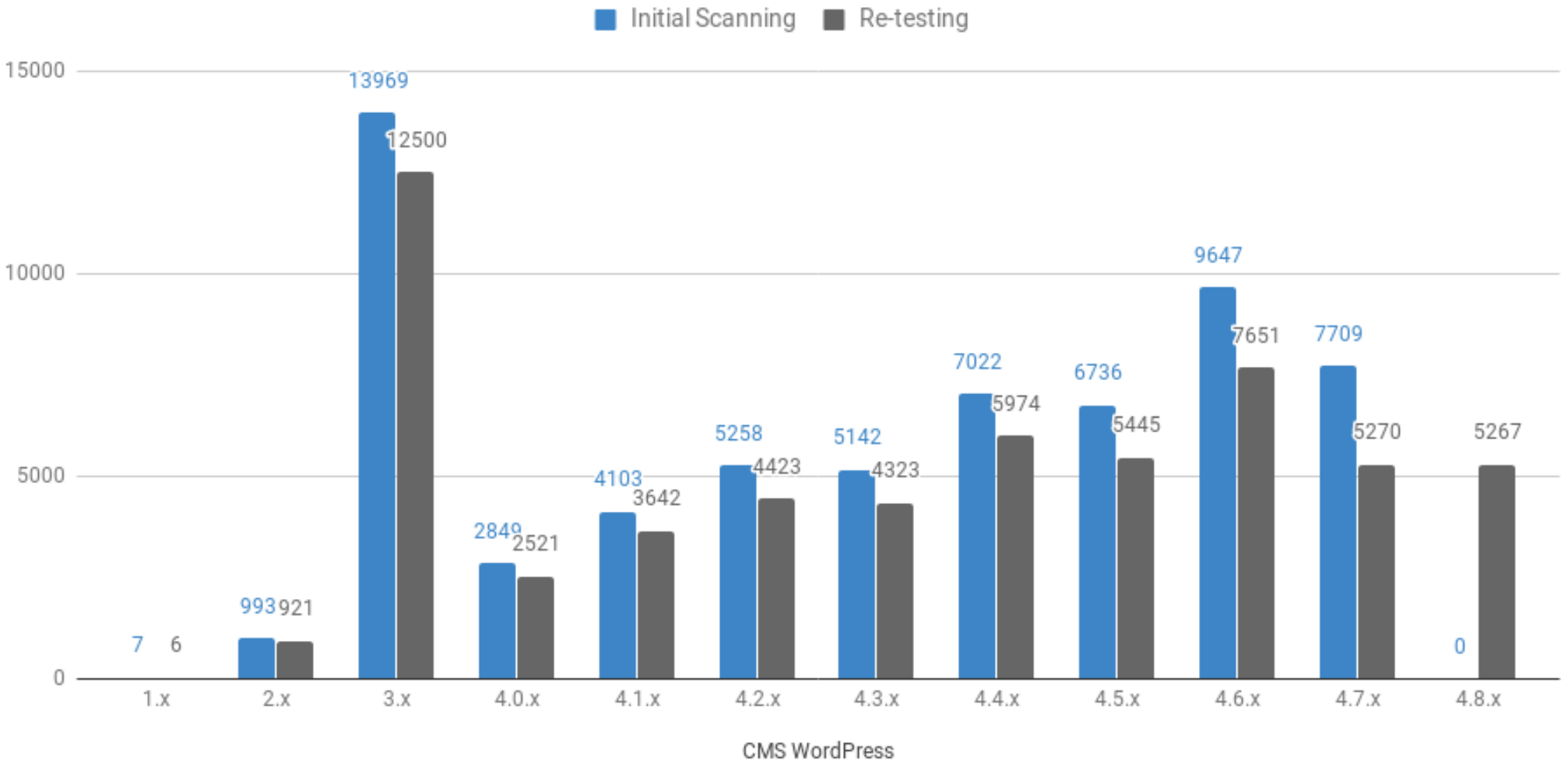
- Script ran from IP 217.31.192.50

  (security research testing host)
- Information was gathered from HTML tag head and its elements

Results

- We identified 50 761 of such domains and informed domain owners
- 25 606 Joomla, 25 155 Wordpress
- Change after 3 weeks from informing users was detected in 10 514 (20,71%)
- People can opt-out from these tests in the future





Lessons learned

- Keep better track of CMS versions
- Don’t run such an actions in summer
- Don’t spend too much time explaining your actions to trolls

Questions?

- **zuzana.duracinska@nic.cz**