Open Source feedback on implementing guidance for NIS 2 security measures

(Source doc) Joint submission by CPANSec, Hackeriet and Markus Knutsen (CISO, Gurusoft AS).

Questionnaire

1. What type of entity are you representing?

□ An entity in scope of these implementing rules
□ An entity in scope of NIS2 but not in scope of these implementing rules
□ [✓ Other]

Please specify: We are two civil society organizations actively involved in several open source software ecosystems. This is a joint response by CPANSec, Hackeriet and Markus Knutsen (CISO, Gurusoft AS).

2. What do you think of the ENISA guidance?

- 1 I like it
- [✓ 2]
- 3 I do not like it

3. Which sections of the guidance do you find most challenging to implement?

These are corresponding to the chapters of the Annex of the implementing regulation.

□ 1. Policy on the security of network and information systems
□ 2. Risk management policy
□ [✓ 3. Incident handling]
□ 4. Business continuity and crisis management
□ 5. Supply chain security
□ [✓ 6. Security in network and information systems acquisition, development and maintenance]
□ 7. Policies and procedures to assess the effectiveness of cybersecurity risk management measures
□ 8. Basic cyber hygiene practices and security training
□ 9. Cryptography
□ 10. Human resources security
□ 11. Access control
□ 12. Asset management
□ 13. Environmental and physical security

Please explain:

General recommendation on chapters 3 and 6 guidance

We reiterate and fully stand behind the general recommendation on chapter 5.1, submitted jointly by OpenSSF, FSFE, NLnet Labs, GitHub and CPANSec, primo December 2024.

Furthermore, it is prudent to emphasize the fact that most software today builds on the rich foundation of infrastructure that has been provided freely by Free and Open Source Software (FOSS) projects and communities. Any incident handling recommendations should explicitly include instructions on how and when to include relevant FOSS maintainers, and clearly raise the point that they, due to the voluntary nature of their role, should to be treated differently than commercial suppliers. The Open Source ecosystems have succeeded due to contributions from their users, and if society is to continue to benefit from this collaboration, it is critical to interact with them in a manner suited for any volunteering community. To help illuminate their special role, it helps to not estrange them as “third-party” suppliers, but instead treat them as “second-party” partners.

Specific recommendations on chapter 3 guidance:

- **3.1.3** Identify and consider all external stakeholders
    - (line 878): «Identify and consider all external stakeholders (e.g. operators, technology suppliers, ***open source project contacts***) necessary for incident handling.»
- **3.2.1** Identify one or more objectives of the monitoring the activities
    - (line 896): Add to the list, «Monitor for new CVE’s issued for any Open Source components used by the entity.»
- **3.2.7** Reviewing of logs
    - (line 1064): Use RFC 3339 instead (not encumbered by license cost)
- **3.5.3** Establish communication plans and procedures
    - (line 1259): Add to «**including Open Source projects**» to end of sentence.
    - (line 1264): Change to «Procedures on how to communicate the incident to customers or how and when to involve a supplier ***or*** **OSS project contact** (if applicable)»
- **3.6.1** Carry out post-incident reviews after recovery from incidents

    - (line 1335): Additional point: Share any relevant findings in the post-incident review with affected stakeholders - e.g. Open Source component maintainers, so they may incorporate any lessons in their work.

Specific recommendations on chapter 6 guidance:

- **6.1** Manage risks stemming from the acquisition of ICT services or ICT products
    - (line 2081): The purchasing process only considers commercial products. The guideline should also take into consideration the acquisition of Open Source components. We recommend adding the following: «**This includes any acquisition processes for selecting Open Source software**».

- Many crucial open source components used today will not conform to the points (a) - (f) in 6.1.2. For example an open source project run by volunteers will often not have defined EOL cycles, thorough documentation beyond a readme file, and will not give security assurances to commercial entities regarding their software. We recommend adding the following points to reflect this reality:

    - (Modify line 2119): **«Criteria for open source components should take into account the voluntary nature of open source projects. Acquirers of such components must constructively engage with project maintainers in addressing Identified security requirements and introducing mitigations and/or improvements. The cost of changes and improvements identified by the acquirer should be borne by the commercial entity, and shared with the Open Source project under their license and terms.**»

    - (New point added after line 2136): «**For ICT services or components where there are no formal tenders with the supplier (for example open source projects), relevant results of internal assessments should be shared upstream to improve the project.**»

- **6.2** Lay down rules for the secure development

    - (line 2210, add new point): «**Where relevant, commercial entities should consider assisting the open source projects that they depend on by introducing SDLC processes suited for the project's way of working**.»

- **6.5** Apply policy and procedures for security testing

    - (add point after line 2524): «**Establish and maintain routines for sharing relevant information with open source projects, including discovered vulnerabilities and the automated tests themselves.**»

    - (add point after line 2553): «**When testing reveals an underlying security issue in an open source component, these findings must be shared with the relevant open source project.**»

    - (add point after line 2553): «**Any automated security tests written for open source components, that have a use case relevant beyond the organisation’s specific needs, should be shared with the relevant open source projects.**»

- **6.6** Apply change management procedures for patch management

    - (add point after line 2623): «**Consider assisting upstream open source projects with ensuring that upgrades happen without issues, for example by using release candidates of open source software during development, and offer feedback about any found issues.**»

4. Are there additional standards that should be included in the ENISA guidance? If yes, which ones?

- RFC 3339, instead of ISO-8601

5. What kind of support do you expect from ENISA in the future?

- We reiterate and fully stand behind the comments to this section, submitted jointly by OpenSSF, FSFE, NLnet Labs, GitHub and CPANSec, primo December 2024

- We would welcome the opportunity to enter into a dialogue with ENISA to further elaborate on these points and to support incident handling and secure software development of and with open source software.