New good practice guide by ENISA on disclosing vulnerabilities

ENISA publishes a good practice guide on vulnerability disclosure, aiming to provide a picture of the challenges the security researchers, the vendors and other involved stakeholders are confronted with when disclosing software/hardware vulnerabilities. The study gives a glimpse into the complex vulnerability disclosure landscape by taking stock of the current situation, identifying the challenges and good practices, and proposes concrete recommendations for improvement.

The main part of the report, describes the main concepts behind vulnerability disclosure along with some figures of the number of vulnerabilities disclosed in the past thirteen (13) years. In continuation the key stakeholders involved in the vulnerability disclosure process along with their roles are defined as well as four (4) case studies of disclosed vulnerabilities.

***Prof. Udo Helmbrecht**, Executive Director of ENISA, commented: "Nowadays vulnerability disclosure implies a lot of complex interdependencies which can be tackled only in coordinated manner by the parties involved in the process". This study is the first attempt to provide a reference guide on the topic of vulnerability disclosure. ENISA welcomes the opportunity to support further work in the field by promoting good practices, increasing awareness, research and further development in this complex domain".*

The gaps commonly found in vulnerability disclosure are related to legal implications, lack of awareness among the stakeholders and difference in maturity levels among vendors and among researchers. Core recommendations for improvement include:

- The community must facilitate the improvement of vendor maturity
- Internationalisation through policy learning, meaning the internet requires a more transnational approach to the topic of vulnerability disclosure, successful stories can be considered.
- Introduction of a neutral third party or enhancement of existing coordination centres.
- European policy makers and Member States should improve the legal framework involved in the disclosure
- Vendors should facilitate trust building, transparency and openness
- ENISA could facilitate and advise to improve the vulnerability disclosure landscape to the community and the European Commission.

In addition, the report offers a 'vulnerability disclosure policy template' providing the procedural steps and timing that can be followed by the constituency in order to implement a vulnerability disclosure policy.

The overall conclusion is that even though there are many positive aspects in the area, there is still room for improvement, which can be identified to an appropriate legal landscape and more trust and transparency between the involved parties.

For full report
For technical information: Cosmin Ciobanu, NIS Expert, **email:** Cosmin.Ciobanu@enisa.europa.eu, **Tel:** +30 2814 409663
For interviews and media inquiries please contact **press@enisa.europa.eu** , **Tel.** +30 2814 409576