**New major incidents in 2012 report by EU cyber security agency ENISA**

**The European Union Agency for Network and Information Security (ENISA) today issued a new report providing an overview of the major outage incidents in the EU in 2012. The aggregated report shows that out of the 79 incidents reports, almost 40% of the incidents affected the possibility of dialling the emergency number “112”. Mobile telephony/mobile Internet was most affected, and disrupted communications for millions of users.**

The *Annual Incident Reports 2012* publication covers the year’s major security incidents in the EU. It provides an aggregated analysis of the 79 reported incidents of severe outages of electronic communication networks, or services. Key conclusions include:

* 18 countries reported 79 significant incidents, nine countries reported no significant incidents.
* Most incidents affected mobile telephony or mobile internet (about 50%).
* Incidents affecting mobile telephony or mobile internet also affected most users (around 1,8 million users per incident). This is consistent with the high penetration rate of mobile telephony and mobile internet in the EU.
* Incidents caused by overload followed by power failures respectively had most impact in terms of number of users affected times duration.
* For most incident reports, as well as for the four services, (fixed and mobile telephony, and fixed and mobile internet) the root cause was “System failures” (75 %).
* Hardware failures were the most common cause of “Systems failures”, followed by software bugs.
* Switches were the most frequent point of failure (e.g. routers and local exchange points) followed by mobile network home location registers.
* Root cause third party failure incidents, mostly power supply failures, affected around 2.8 million users on average.
* Incidents involving overload affected around 9.4 million users on average.
* Incidents caused by natural phenomena (mainly storms and heavy snowfall) lasted the longest: on average around 36 hours.

Anonymized examples of the incidents reported range from:

* Overload causing VoIP outage
* Faulty upgrade halting IP-based traffic
* Cable theft causing fibre optic cable break
* Distributed Denial of Service (DDoS) attacks on Domain Name System (DNS) affecting mobile internet
* Faulty software update affecting mobile telephony

The Executive Director of ENISA Professor Udo Helmbrecht commented:

*“The EU collaboration behind this report is key to improving the security and resilience of electronic communications networks in the EU, as well as for security in other critical sectors*. Reporting major incidents helps us understand what went wrong, why, and how to prevent similar incidents from happening again. ENISA, with all National Reporting Authorities across the EU, will continue delivering practical lessons learned, that could significantly improve the security of our telecommunication infrastructure.”

The next annual (2013) report will be published in spring, 2014.

**For full report;** [Annual Incidents Report 2012](https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2012/)

**Background:** Article 13a of the [Framework Directive (2009/140/EC)](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32009L0140:en:NOT) in the [EU legal framework for electronic communications](http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf).

**For interviews, contact:** Ulf Bergström, Public Affairs Unit, Mobile: (+30) 6948460143, e-mail: [ulf.bergstrom@enisa.europa.eu](mailto:ulf.bergstrom@enisa.europa.eu) ,or resilience@enisa.europa.eu