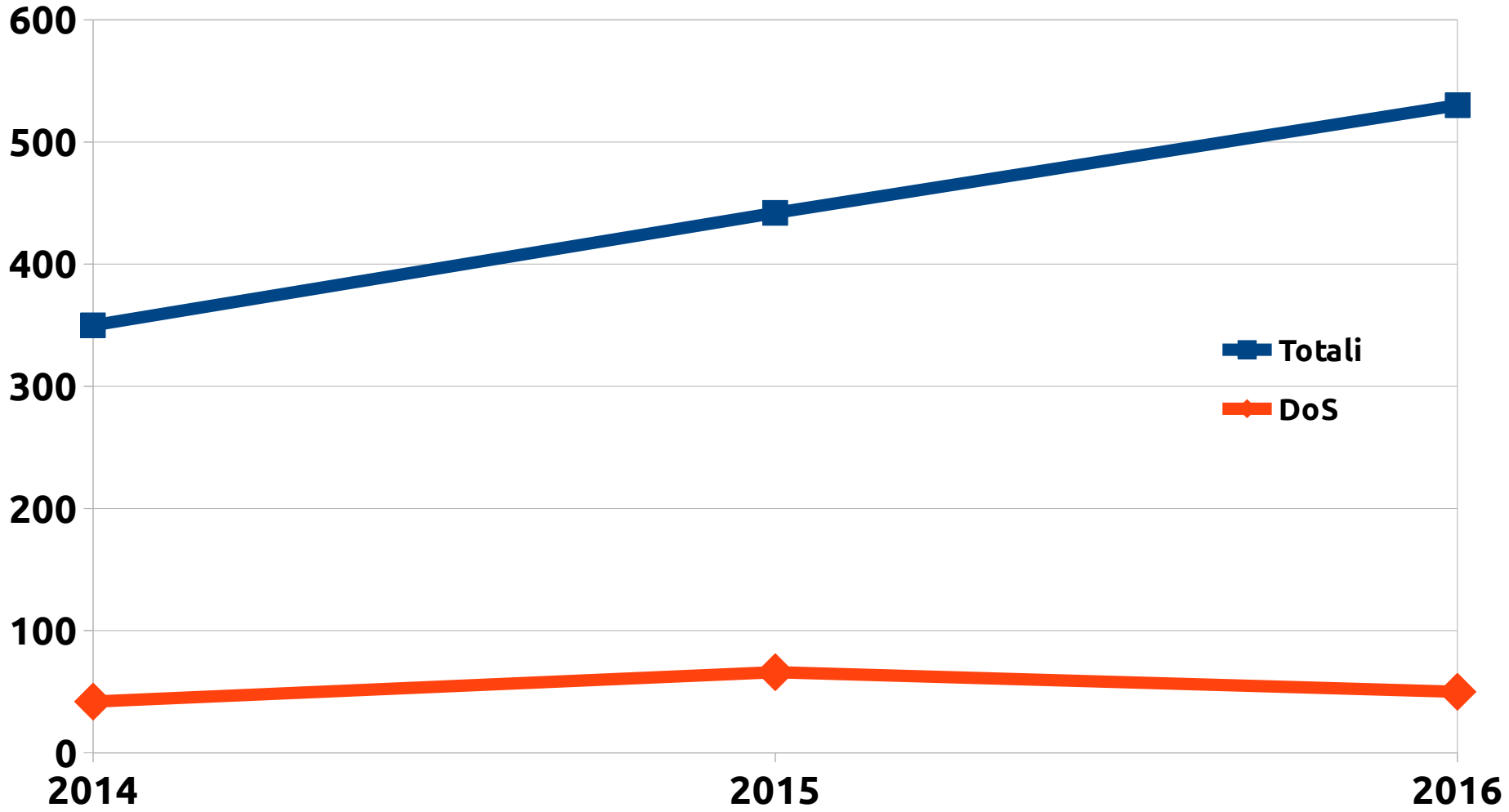
Rapporto dal gruppo Auditing

Riunione di CCR
Lecce, 12-14 Settembre 2016

Gruppo auditing

- Membri
  - Franco Brasolin
  - Roberto Cecchini
  - Leandro Lanzi
  - Antonella Monducci
  - Michele Michelotto
- **https://audiweb.infn.it/**

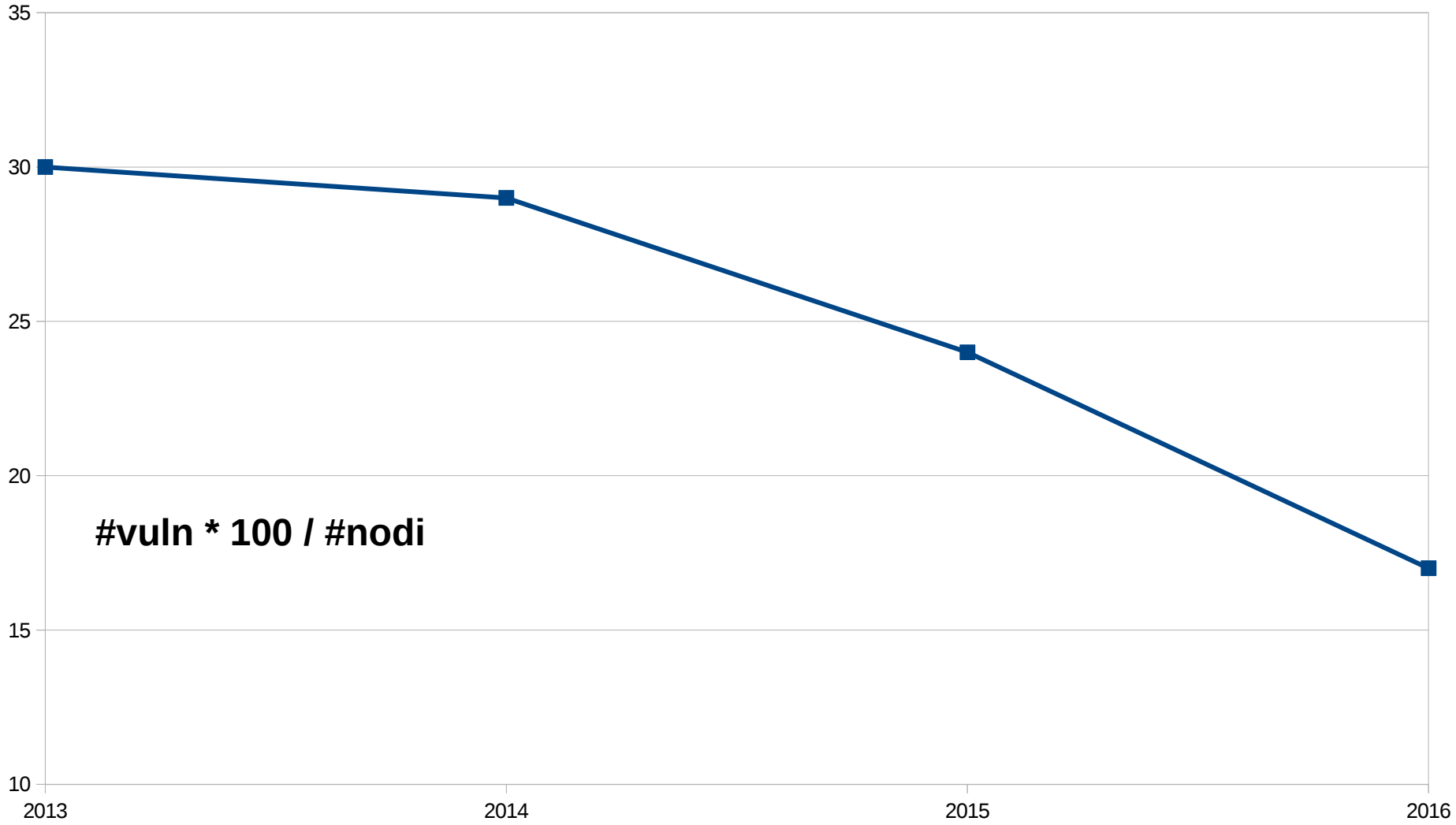
Incidenti di origine INFN



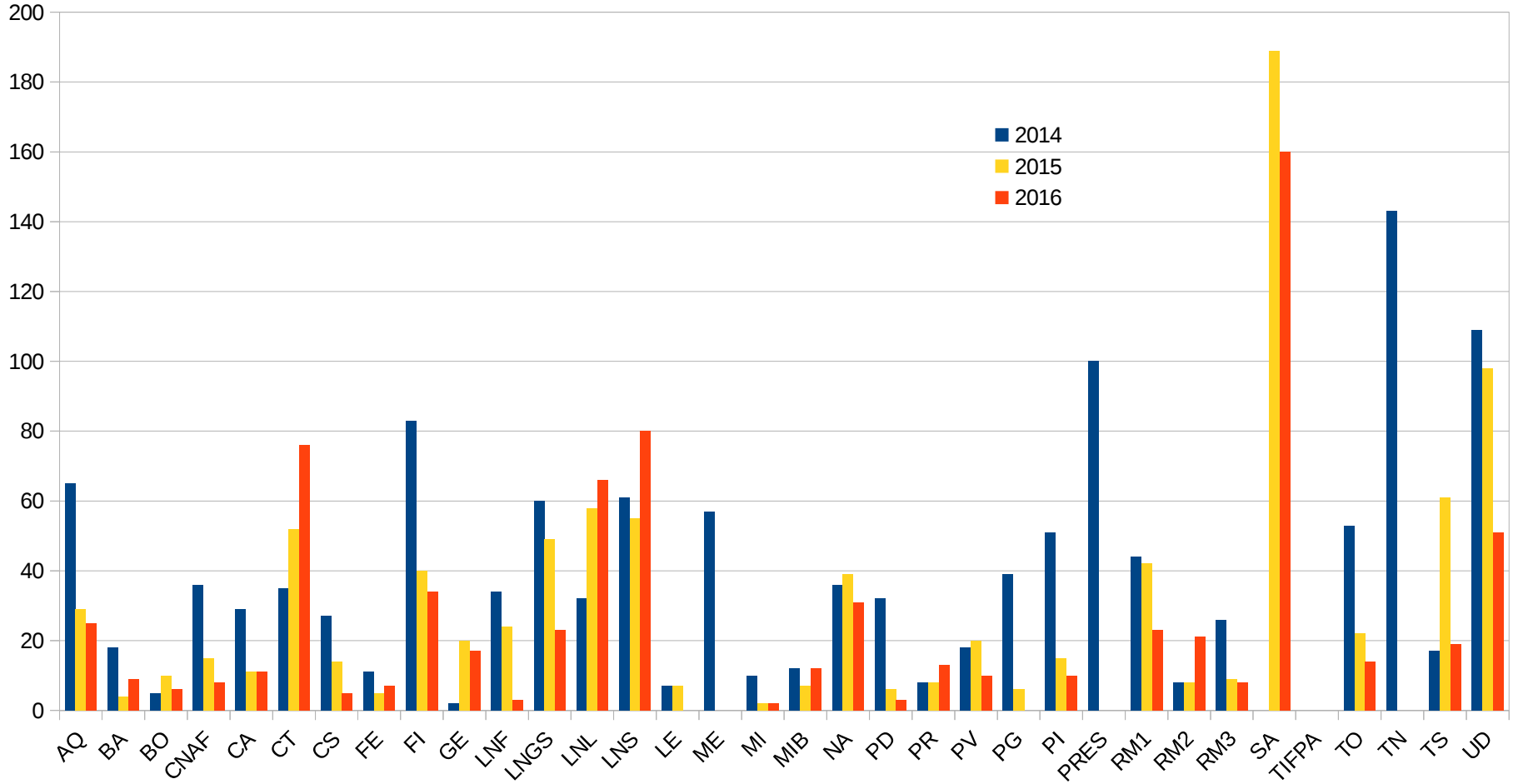
Scansioni periodiche

- Nessus (Professional Feed)
- Numero nodi esaminati:
  - 2013: 3137
  - 2014: 3928
  - 2015: 3479
  - **2016: 2697**

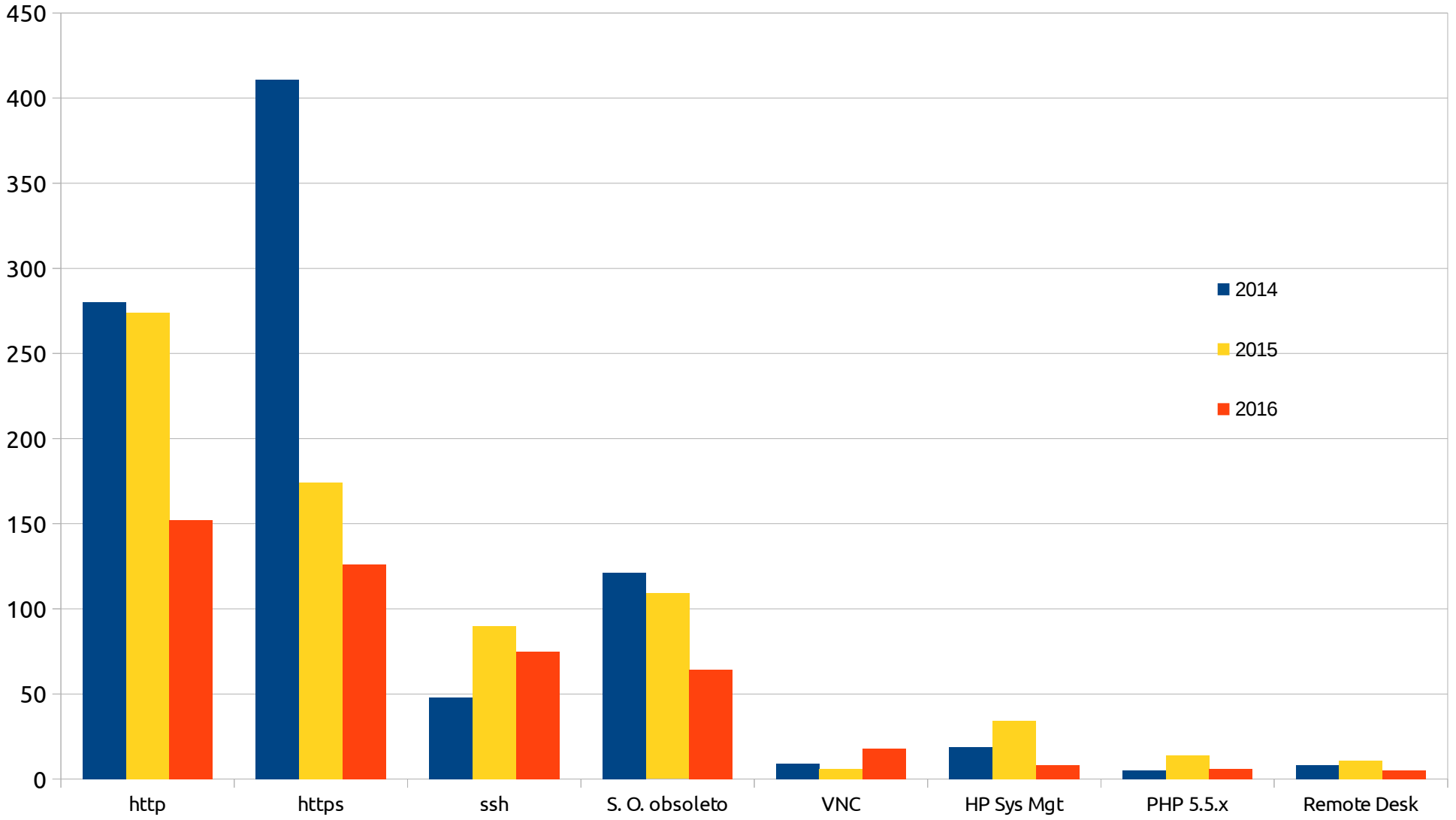
Indice vulnerabilità



Indice vulnerabilità (per Struttura)



Vulnerabilità (per porta)

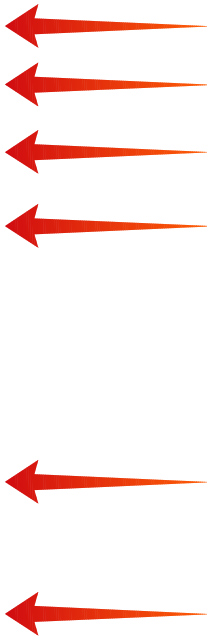


Vulnerabilità (per tipo)

- 60 OpenSSH MaxAuthTries Bypass
- 52 Unsupported Unix Operating System
- 24 Apache HTTP Server Byte Range DoS
- 11 Apache HTTP Server Byte Range DoS
- 8 Apache 2.2.x < 2.2.28 Multiple Vulnerabilities
- 4 OpenSSL 'ChangeCipherSpec' MiTM Vulnerability
- 4 PHP 5.5.x < 5.5.37 Multiple Vulnerabilities
- 3 OpenSSL Heartbeat Information Disclosure (Heartbleed)

Principali porte aperte

Servizio	Porta	# Vuln.	# porte aperte
ssh	22	75 (90)	1265 (1951)
http	80, 8000, 8080	152 (274)	774 (931)
https	443, 8443	126 (174)	635 (738)
mysql	3306		126 (212)
printer	631, 515, 9100		32 (193)
VNC	5900-3	18 (5)	134 (132)
ganglia	8649		72 (151)
nrpe (nagios)	5666	2 (39)	52 (116)
smtp	25	3 (3)	84 (102)
domain	53		73 (83)
sunrpc	111		15 (25)
x11	6000	2 (-)	30 (32)
ftp	21		10 (15)
tftp	69/u		2 (1)
shell / rsh	514	- (1)	6 (4)



Server Web

- Porta 80: **517**
  - Cisco IOS http config: 7
  - stampanti: ≥ 26
- Porta 443: **376**
  - Cisco IOS http config: 6
  - Cisco ASA fw config: 2
  - stampanti: ≥ 16

https

- 35 server “primari”
  - 14 non esistono o sono altra cosa
  - verifica con **v.gd/YACdaO**
    - 3 A: Bologna, CNAF, Milano
    - 4 B
    - 10 C
    - **4 F** (!)
      - OpenSSL Padding Oracle & poodle
- Perché non passare ad https?
  - prestazioni: https://www.httpvshttps.com/

Scalare la classifica

- **Aggiornare openSSL!**
- apache (**`ssl.conf`**)

  `SSLProtocol all -SSLv3 -SSLv2`
- postfix (**`main.cf`**)

  `smtpd_tls_mandatory_protocols=!SSLv2, !SSLv3`
- dovecot (**`/etc/dovecot/conf.d/10-ssl.conf`**)

  `ssl_protocols = !SSLv3 !SSLv2`
- **http://v.gd/gFhBHH**

INFN CA

- Certificati INFN validi (al 30/9/2016)
  - personali: 1396
  - server: 677
  - servizio: 12
  - robot: 15
- **Perché non passare al servizio TCS?**
- **Quali usi non sono gestibili con certificati TCS?**

Tipologia incidenti

Applicazioni Web	**30%**
Errori vari	**27%**
Furto credenziali	**17%**
Altro	**26%**

Fonte: Verizon, 2016 Data Breach Investigation

Varie & eventuali

- Corso sicurezza siti web
  - 20 – 22 Settembre, Firenze (ancora 10 posti)
- DNSSec
- Altri tool analisi