Top Level Domain Security Checklist
Presented by Martin Lindner
Focus of Presentation

• This presentation is focusing on proper configuration and deployment of TLD name servers.

• This presentation does not address physical security, hardening of operating systems or data integrity between registrars and registries.
Security Checklist for Top Level Domains

- Software version
- Recursion
- SOA records
- Consistent NS records
- Authoritative answers
- Restricted zone transfers
- Name servers on multiple networks
Software version

✅ Does the name server software have known vulnerabilities?

✅ Is someone monitoring for new threats and vulnerabilities?
  • CERT/CC Advisories
  • Vendor Advisories
  • Public news groups and mailing lists
Recursion

✔ Do the name servers use recursion?
   • Recursion leaves name servers vulnerable to cache poisoning.
Do the name servers have a Start of Authority (SOA) record for the TLD?
Consistence NS records

- Do all the name servers listed in the root answer authoritative for the TLD?
  - Lame Delegations

- Do the name servers’ NS records match the NS records offered by the root?
Authoritative answers

Do the name servers give authoritative answers?

✓
Restricted Zone Transfers

✓ Do the name servers restrict zone transfers to authorized parties?
DNS on multiple networks

✔ Are name servers distributed across multiple networks?
  • Different networks
  • Multiple upstream providers
One or more servers non-compliant
Unknown status
All servers compliant

Software Version - 27
Recursion Disabled - 47
Restricted Zone Transfers - 97
Consistent NS Records - 106
Authoritative Answers - 171
SOA Records - 183
Name Servers on multiple networks - 242
CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh PA 15213-3890
USA

Hotline: +1 412 268 7090   CERT personnel answer 8:00 a.m. — 5:00 p.m. EST(GMT-5) / EDT(GMT-4), and are on call for emergencies during other hours.

Fax: +1 412 268 6989

Web: http://www.cert.org/

Email: cert@cert.org