Prioritization

The following list provides expected prioritization per issue for the given scenario. If good reasoning is given, the prioritization can be different.

- 51956 MS11-004: False positive (patched in meantime)

  – Critical: 50% (correct priority, but false positive was not detected)

- 97833 MS17-010: Medium / High (can only be reached via Sys Admin network which is highly trusted)
- 26919 SMB Guest Account: Low / Medium (only reachable via Sys Admin Network)
- 10166 FTP Guest Account: False positive

  – High / Critical: 50% (correct priority)

- 10079 Anonymous FTP account: Critical

  – Bonus point if medical data has been found

- 62940 Information Disclosure in FTP: Medium

  – Argument for High can be accepted

- 90510 Badlock vulnerability: Low / Medium (only reachable via Sys Admin Network)
- 57608 SMB signing not required: Low / Medium (only reachable via Sys Admin Network)

Other issues such as 34324 FTP Cleartext can be classified higher (bonus points for good arguments according to business scenario).

Immediate actions

- Install patch for MS11-004 is installed (unless detected as false positive)
- Install patch for MS17-010
- Disable anonymous FTP access

Mid-term actions

- Get rid of plaintext authentication
- Switch FTP for something encrypted
- Implement VPN or whitelisted FW access (not feasible immediate)