

# ISO/IEC TR 20004:2015-12 (E)

## Information technology - Security techniques - Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045

---

<b>Contents</b>	<b>Page</b>
Foreword .....	iv
Introduction .....	v
1 Scope .....	1
2 Terms and definitions .....	1
3 Abbreviated terms .....	3
4 Background context .....	4
5 Vulnerability assessment activities .....	8
5.1 Determine relevant potential vulnerabilities .....	9
5.1.1 Identify relevant weaknesses and attack patterns from existing structured assurance case .....	11
5.1.2 Identify relevant weaknesses and attack patterns from public sources .....	11
5.2 Assess TOE susceptibility to attack .....	14
5.2.1 Design and specify security/penetration testing .....	14
5.2.2 Execute and document security/penetration testing .....	15
5.3 Report on exploitable vulnerabilities .....	15
Bibliography .....	17