

ISO/IEC TR 20004:2012-08 (E)

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

Contents		Page
Foreword		iv
Introduction		v
1	Scope	1
2	Terms and definitions	1
3	Abbreviated terms	3
4	Background Context	4
5	Overview	9
5.1	Purpose	9
6	Vulnerability Assessment Activities	10
6.1	Determine relevant potential vulnerabilities	10
6.1.1	Identify relevant weaknesses and attack patterns from existing structured assurance case	12
6.1.2	Identify relevant weaknesses and attack patterns from public sources	12
6.2	Assess TOE susceptibility to attack	15
6.2.1	Design and specify security/penetration testing	15
6.2.2	Execute and document security/penetration testing	15
6.3	Report on exploitable vulnerabilities	16
Bibliography		17