

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