ISO/IEC 30111:2019-10 (E)

Information technology - Security techniques - Vulnerability handling processes

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Termsanddefinitions 1

4 Abbreviated terms 1

5 Relationships to other International Standards 1

6 Policy and organizational framework 3
6.1 General 3
6.2 Leadership 3
6.2.1 Leadership and commitment 3
6.2.2 Policy 3
6.2.3 Organizational roles, responsibilities, and authorities 4
6.3 Vulnerability handling policy development 4
6.4 Organizational framework development 4
6.5 Vendor CSIRT or PSIRT 5
6.5.1 General 5
6.5.2 PSIRT mission 5
6.5.3 PSIRT responsibilities 5
6.5.4 Staff capabilities 6
6.6 Responsibilities of the product business division 6
6.7 Responsibilities of customer support and public relations 7
6.8 Legal consultation 7

7 Vulnerability handling process 7
7.1 Vulnerability handling phases 7
7.1.1 General 7
7.1.2 Preparation 8
7.1.3 Receipt 8
7.1.4 Verification 9
7.1.5 Remediation development 10
7.1.6 Release 10
7.1.7 Post-release 10
7.2 Process monitoring 11
7.3 Confidentiality of vulnerability information 11

8 Supply chain considerations 11

Bibliography 13