

E DIN EN ISO/IEC 29147:2020-01 (E)

Erscheinungsdatum: 2019-12-06

Information technology - Security techniques - Vulnerability disclosure (ISO/IEC 29147:2018); English version prEN ISO/IEC 29147:2020

Contents

Page

Foreword.....	vi
Introduction.....	vii
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms	3
5 Concepts	3
5.1 General.....	3
5.2 Structure of this document.....	3
5.3 Relationships to other International Standards.....	4
5.3.1 ISO/IEC 30111.....	4
5.3.2 ISO/IEC 27002.....	5
5.3.3 ISO/IEC 27034 series.....	6
5.3.4 ISO/IEC 27036-3.....	6
5.3.5 ISO/IEC 27017.....	6
5.3.6 ISO/IEC 27035 series.....	6
5.3.7 Security evaluation, testing and specification.....	6
5.4 Systems, components, and services.....	6
5.4.1 Systems.....	6
5.4.2 Components.....	6
5.4.3 Products.....	6
5.4.4 Services.....	7
5.4.5 Vulnerability.....	7
5.4.6 Product interdependency.....	7
5.5 Stakeholder roles.....	8
5.5.1 General.....	8
5.5.2 User.....	8
5.5.3 Vendor.....	8
5.5.4 Reporter.....	8
5.5.5 Coordinator.....	9
5.6 Vulnerability handling process summary.....	9
5.6.1 General.....	9
5.6.2 Preparation.....	10
5.6.3 Receipt.....	10
5.6.4 Verification.....	11
5.6.5 Remediation development.....	11
5.6.6 Release.....	11
5.6.7 Post-release.....	12
5.6.8 Embargo period.....	12
5.7 Information exchange during vulnerability disclosure.....	12
5.8 Confidentiality of exchanged information.....	13
5.8.1 General.....	13
5.8.2 Secure communications.....	13
5.9 Vulnerability advisories.....	13
5.10 Vulnerability exploitation.....	14
5.11 Vulnerabilities and risk.....	14

6	Receiving vulnerability reports	14
6.1	General	14
6.2	Vulnerability reports	14
6.2.1	General	14
6.2.2	Capability to receive reports	14
6.2.3	Monitoring	15
6.2.4	Report tracking	15
6.2.5	Report acknowledgement	15
6.3	Initial assessment	16
6.4	Further investigation	16
6.5	On-going communication	16
6.6	Coordinator involvement	16
6.7	Operational security	17
	Publishing vulnerability advisories	17
7.1	General	17
7.2	Advisory	17
7.3	Advisory publication timing	17
7.4	Advisory elements	18
7.4.1	General	18
7.4.2	Identifiers	18
7.4.3	Date and time	18
7.4.4	Title	19
7.4.5	Overview	19
7.4.6	Affected products	19
7.4.7	Intended audience	19
7.4.8	Localization	19
7.4.9	Description	19
7.4.10	Impact	19
7.4.11	Severity	20
7.4.12	Remediation	20
7.4.13	References	20
7.4.14	Credit	20
7.4.15	Contact information	20
7.4.16	Revision history	20
7.4.17	Terms of use	20
7.5	Advisory communication	20
7.6	Advisory format	21
7.7	Advisory authenticity	21
7.8	Remediations	21
7.8.1	General	21
7.8.2	Remediation authenticity	21
7.8.3	Remediation deployment	21
	Coordination	21
8.1	General	21
8.2	Vendors playing multiple roles	22
8.2.1	General	22
8.2.2	Vulnerability reporting among vendors	22
8.2.3	Reporting vulnerability information to other vendors	22
	Vulnerability disclosure policy	22
9.1	General	22
9.2	Required policy elements	23
9.2.1	General	23
9.2.2	Preferred contact mechanism	23
9.3	Recommended policy elements	23
9.3.1	General	23

9.3.2	Vulnerability report contents.....	23
9.3.3	Secure communication options.....	24
9.3.4	Setting communication expectations.....	24
9.3.5	Scope.....	24
9.3.6	Publication.....	24
9.3.7	Recognition.....	24
9.4	Optional policy elements.....	24
9.4.1	General.....	24
9.4.2	Legal considerations.....	24
9.4.3	Disclosure timeline.....	24
Annex A (informative) Example vulnerability disclosure policies.....		25
Annex B (informative) Information to request in a report.....		26
Annex C (informative) Example advisories.....		27
Annex D (informative) Summary of normative elements.....		30
Bibliography.....		32