

# DIN EN ISO/IEC 29147:2020-08 (E)

## Information technology - Security techniques - Vulnerability disclosure (ISO/IEC 29147:2018)

---

<b>Contents</b>		<b>Page</b>
European foreword.....		5
Foreword.....		6
Introduction.....		7
<b>1</b>	<b>Scope</b> .....	<b>8</b>
<b>2</b>	<b>Normative references</b> .....	<b>8</b>
<b>3</b>	<b>Terms and definitions</b> .....	<b>8</b>
<b>4</b>	<b>Abbreviated terms</b> .....	<b>10</b>
<b>5</b>	<b>Concepts</b> .....	<b>10</b>
5.1	General.....	10
5.2	Structure of this document.....	11
5.3	Relationships to other International Standards.....	11
5.3.1	ISO/IEC 30111.....	11
5.3.2	ISO/IEC 27002.....	12
5.3.3	ISO/IEC 27034 series.....	13
5.3.4	ISO/IEC 27036-3.....	13
5.3.5	ISO/IEC 27017.....	13
5.3.6	ISO/IEC 27035 series.....	13
5.3.7	Security evaluation, testing and specification.....	13
5.4	Systems, components, and services.....	13
5.4.1	Systems.....	13
5.4.2	Components.....	13
5.4.3	Products.....	13
5.4.4	Services.....	14
5.4.5	Vulnerability.....	14
5.4.6	Product interdependency.....	14
5.5	Stakeholder roles.....	15
5.5.1	General.....	15
5.5.2	User.....	15
5.5.3	Vendor.....	15
5.5.4	Reporter.....	15
5.5.5	Coordinator.....	16
5.6	Vulnerability handling process summary.....	16
5.6.1	General.....	16
5.6.2	Preparation.....	17
5.6.3	Receipt.....	17
5.6.4	Verification.....	18
5.6.5	Remediation development.....	18
5.6.6	Release.....	18
5.6.7	Post-release.....	19
5.6.8	Embargo period.....	19
5.7	Information exchange during vulnerability disclosure.....	19
5.8	Confidentiality of exchanged information.....	20
5.8.1	General.....	20
5.8.2	Secure communications.....	20
5.9	Vulnerability advisories.....	20
5.10	Vulnerability exploitation.....	21
5.11	Vulnerabilities and risk.....	21

<b>6</b>	<b>Receiving vulnerability reports</b>	<b>21</b>
6.1	General	21
6.2	Vulnerability reports	21
6.2.1	General	21
6.2.2	Capability to receive reports	21
6.2.3	Monitoring	22
6.2.4	Report tracking	22
6.2.5	Report acknowledgement	22
6.3	Initial assessment	23
6.4	Further investigation	23
6.5	On-going communication	23
6.6	Coordinator involvement	23
6.7	Operational security	24
<b>7</b>	<b>Publishing vulnerability advisories</b>	<b>24</b>
7.1	General	24
7.2	Advisory	24
7.3	Advisory publication timing	24
7.4	Advisory elements	25
7.4.1	General	25
7.4.2	Identifiers	25
7.4.3	Date and time	25
7.4.4	Title	26
7.4.5	Overview	26
7.4.6	Affected products	26
7.4.7	Intended audience	26
7.4.8	Localization	26
7.4.9	Description	26
7.4.10	Impact	26
7.4.11	Severity	27
7.4.12	Remediation	27
7.4.13	References	27
7.4.14	Credit	27
7.4.15	Contact information	27
7.4.16	Revision history	27
7.4.17	Terms of use	27
7.5	Advisory communication	27
7.6	Advisory format	28
7.7	Advisory authenticity	28
7.8	Remediations	28
7.8.1	General	28
7.8.2	Remediation authenticity	28
7.8.3	Remediation deployment	28
<b>8</b>	<b>Coordination</b>	<b>28</b>
8.1	General	28
8.2	Vendors playing multiple roles	29
8.2.1	General	29
8.2.2	Vulnerability reporting among vendors	29
8.2.3	Reporting vulnerability information to other vendors	29
<b>9</b>	<b>Vulnerability disclosure policy</b>	<b>29</b>
9.1	General	29
9.2	Required policy elements	30
9.2.1	General	30
9.2.2	Preferred contact mechanism	30

9.3	Recommended policy elements.....	30
9.3.1	General.....	30
9.3.2	Vulnerability report contents.....	30
9.3.3	Secure communication options.....	31
9.3.4	Setting communication expectations.....	31
9.3.5	Scope.....	31
9.3.6	Publication.....	31
9.3.7	Recognition.....	31
9.4	Optional policy elements.....	31
9.4.1	General.....	31
9.4.2	Legal considerations.....	31
9.4.3	Disclosure timeline.....	31
<b>Annex A (informative) Example vulnerability disclosure policies.....</b>		<b>32</b>
<b>Annex B (informative) Information to request in a report.....</b>		<b>33</b>
<b>Annex C (informative) Example advisories.....</b>		<b>34</b>
<b>Annex D (informative) Summary of normative elements.....</b>		<b>37</b>
<b>Bibliography.....</b>		<b>39</b>