# ISO/IEC 29147:2018 (E)

## Information technology — Security techniques — Vulnerability disclosure

# Contents


Foreword

Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 Abbreviated terms

5 Concepts

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

6 Receiving vulnerability reports

6.1 General

6.2 Vulnerability reports
6.2.1 General
6.2.2 Capability to receive reports
6.2.3 Monitoring
6.2.4 Report tracking
6.2.5 Report acknowledgement
6.3 Initial assessment
6.4 Further investigation
6.5 On-going communication
6.6 Coordinator involvement
6.7 Operational security

7 Publishing vulnerability advisories

7.1 General
7.2 Advisory
7.3 Advisory publication timing
7.4 Advisory elements
7.4.1 General
7.4.2 Identifiers
7.4.3 Date and time
7.4.4 Title
7.4.5 Overview
7.4.6 Affected products
7.4.7 Intended audience
7.4.8 Localization
7.4.9 Description
7.4.10 Impact
7.4.11 Severity
7.4.12 Remediation
7.4.13 References
7.4.14 Credit
7.4.15 Contact information
7.4.16 Revision history
7.4.17 Terms of use
7.5 Advisory communication
7.6 Advisory format
7.7 Advisory authenticity
7.8 Remediations
7.8.1 General
7.8.2 Remediation authenticity
7.8.3 Remediation deployment

8 Coordination

8.1 General
8.2 Vendors playing multiple roles
8.2.1 General
8.2.2 Vulnerability reporting among vendors
8.2.3 Reporting vulnerability information to other vendors

9 Vulnerability disclosure policy

9.1 General
9.2 Required policy elements
9.2.1 General
9.2.2 Preferred contact mechanism
9.3 Recommended policy elements
9.3.1 General
9.3.2 Vulnerability report contents
9.3.3 Secure communication options
9.3.4 Setting communication expectations
9.3.5 Scope
9.3.6 Publication
9.3.7 Recognition
9.4 Optional policy elements
9.4.1 General

9.4.2 Legal considerations
9.4.3 Disclosure timeline

Annex A (informative) Example vulnerability disclosure policies

A.1 Facebook
A.2 CERT/CC
A.3 Zero Day Initiative
A.4 Cisco
A.5 NCSC-FI
A.6 NCSC-NL
A.7 Rapid7

Annex B (informative) Information to request in a report

Annex C (informative) Example advisories

C.1 Example advisory
C.2 Heap memory corruption in ASN.1 parsing code generated by Objective Systems Inc. ASN1C compiler for C/C++
C.3 Multiple Vulnerabilities in Network Time Protocol Daemon Affecting Cisco Products: November 2016
C.4 RHSA-2017:0057 — Security Advisory
C.5 Alert (TA10-159A) Adobe Flash, Reader, and Acrobat Vulnerability

Annex D (informative) Summary of normative elements

Page count: 32