

ISO/IEC TR 5895:2022-06 (E)

Cybersecurity - Multi-party coordinated vulnerability disclosure and handling

Contents		Page
Foreword.....		v
Introduction.....		vi
1	Scope.....	1
2	Normative references.....	1
3	Terms and definitions.....	1
4	Concepts.....	1
4.1	General.....	1
4.2	Relationship with other International Standards.....	3
4.2.1	ISO/IEC 29147 - Vulnerability disclosure.....	3
4.2.2	ISO/IEC 30111 - Vulnerability handling processes.....	3
4.2.3	Risk reduction effectiveness.....	4
5	MPCVD scenarios.....	5
5.1	General.....	5
5.2	MPCVD led by the vendor-coordinator (the owner of the technology developed) – the “mitigating vendor”.....	5
5.3	MPCVD process in non-owner cases.....	5
6	MPCVD stakeholders.....	5
6.1	General.....	5
6.2	Vendor.....	5
6.2.1	Mitigating vendor.....	5
6.2.2	Dependent vendor.....	6
6.2.3	Mitigating vendor and coordination.....	6
6.3	Non-vendor coordinator.....	6
6.4	Reporters.....	6
6.5	Users.....	6
6.6	Product security incident response team (PSIRT) function.....	6
7	MPCVD life cycle.....	6
7.1	General.....	6
7.2	Policy development.....	7
7.2.1	Preparation.....	7
7.2.2	Policy.....	7
7.3	Strategy development.....	7
7.3.1	Information sharing strategy.....	7
7.3.2	Disclosure strategy.....	7
7.4	Know your customers.....	8
7.5	Encrypted communication methods and conference calls.....	8
7.6	Processes and controls.....	8
8	MPCVD life cycle for each product.....	8
8.1	Product and user mapping.....	8
8.2	Component analysis.....	8
8.3	User analysis.....	9
9	MPCVD life cycle for each vulnerability.....	9
9.1	Receipt.....	9
9.2	Verification.....	9
9.3	Remediation development.....	10

9.4	Release.....	10
9.5	Post-release.....	10
9.6	Embargo period.....	10
10	Information exchange.....	11
11	Disclosure.....	12
12	Use case for hardware and further considerations.....	12
	Bibliography.....	14