ETSI TR 104 003 V1.1.1 (2024-09)

Cyber Security (CYBER);
The vulnerability disclosure ecosystem

Reference
DTR/CYBER-00118

Keywords
cybersecurity, resilience

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

ENISA's 2018 exhaustive study on the Economics of Vulnerability Disclosure [i.17] concluded with the finding that "emphasizes the importance of approaching vulnerability disclosure as an ecosystem". The ecosystem is also the product of a complex history beginning in 1967.

Introduction

The present document provides a comprehensive treatment of the vulnerability disclosure ecosystem - which has grown in fundamental importance for cyber security risk management. It also seeks to bridge the widely prevalent institutional/national/sector insularity which exists.

Much of the history of vulnerability disclosure remains uncaptured - together with the emergence and evolution of the ecosystem. The ecosystem is rapidly growing in complexity. New platforms and protocols have been developed. New marketplace participants have emerged, and new regulatory regimes are appearing. Subject matter is now threaded through SBOM/supply chain risk management, resilience, Zero Trust Model, and automated security control capabilities.

Emerging challenges are largely unrecognized and deserve being addressed. The Technical Report is additionally aimed at supporting related needs of ETSI members, EU/CEPT government bodies, SMEs and consumers; including potential future ETSI TC CYBER actions.

1 Scope

The present document provides an overview of the history and facets of the cyber vulnerability disclosure ecosystem. The overview includes the history of this activity, the concepts and specifications that emerged, the diverse venues and use cases, imposed obligations, and the technological and social challenges faced.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

[i.2] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

[i.3] Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020.

[i.4] Commission Implementing Decision of XXX on a standardisation request to the [European Standards Organisations] in support of Union policy on horizontal cybersecurity requirements for products with digital elements Version of DD of Month YYYY.

[i.5] Office of the Central Cyberspace Affairs Commission: "Ministry of Industry and Information Technology Cyberspace Administration of China Notice of the Ministry of Public Security on Printing and Distributing Regulations on the Management of Security Vulnerabilities in Network Products".

[i.6] GCHQ: "The Equities Process".

[i.7] Vulnerabilities Equities Policy and Process for the United States Government.

[i.8] ETSI TR 103 305 (all parts): "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence".

[i.9] ETSI TR 103 838: "Cyber Security; Guide to Coordinated Vulnerability Disclosure".

[i.10] ETSI TS 102 165-1: "CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)".

[i.11] CVE® Program Mission.

[i.12] GSMA FS.23: "GSMA Coordinated Vulnerability Disclosure Program".

[i.13] FIRST: "Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure".

[i.14] NIST SP 800-30: "Guide for Conducting Risk Assessments".

[i.15] NTIA: "Multistakeholder Process: Cybersecurity Vulnerabilities".

[i.16] CISA: "Software Bill of Materials".

[i.17] ENISA: "Economics of vulnerability disclosure".

[i.18] ENISA: "Telecom Security Incidents 2021: Annual Report", July 2022.

[i.19] SecurityScorecard: "CVE Details".

[i.20] FIRST - Exploit Prediction Scoring System: "EPSS Data".

[i.21] CISA: "Reducing the Significant Risk of Known Exploited Vulnerabilities".

[i.22] Wikipedia: "Market for zero-day exploits".

[i.23] Zhang et al.: "An Empirical Study on Using the National Vulnerability Database to Predict Software Vulnerabilities," Database and Expert Systems Applications - 22nd International Conference, DEXA 2011, Toulouse, France, August 29 - September 2, 2011.

[i.24] CyberRisk Alliance: "Listen: Former NSA analyst Tony Sager tackled 'fog of more".

[i.25] ENISA "Coordinated Vulnerability Disclosure Policies in the EU".

[i.26] Leadbeater, NFV World Congress, "Introduction to NFV SEC WG & NFV Security Challenges".

[i.27] CISA: "Zero Trust Maturity Model".

[i.28] CISA: "Known Exploited Vulnerabilities Catalog".

[i.29] NTIA: "Roles and Benefits for SBOM Across the Supply Chain".

[i.30] OECD: "Working Party on Security in the Digital Economy, Encouraging Vulnerability Treatment, Responsible management, handling and disclosure of vulnerabilities".

[i.31] CERT/CC: "Designing Vultron: A Protocol for Multi-Party Coordinated Vulnerability Disclosure (MPCVD)".

[i.32] NCSC: "Device Security Guidance".

[i.33] BSI: "SBOM-Anforderungen: TR-03183-2 stärkt Sicherheit in der Software-Lieferkette".

[i.34] ODNI, CISA, NSA, "Securing the Software Supply Chain: Recommended Practices for Software Bill of Materials Consumption".

[i.35] Cloud Security Alliance, Global Security Database: "Getting Started".

[i.36] Jake Edge: "Resurrecting DWF".

[i.37] The Daily Swig: "Latest Internet of Things (IoT) security news".

[i.38] RAND Memorandum RM-3765-PR (August 1964): "On Distributed Communications - IX. Security Secrecy and Tamper-Free Considerations", Paul Baran,. https://www.rand.org/content/dam/rand/pubs/research_memoranda/2006/RM3767.pdf.

[i.39] Software Engineering Institute: "Prioritizing Vulnerability Response: A Stakeholder-Specific Vulnerability Categorization (Version 2.0)".

[i.40] NIST NVD Program Announcements.

[i.41] NVD Data Overrides.

[i.42] CVE Mission Program.

[i.43] CISA Vulnrichment.

[i.44] ENISA: "Vulnerability Disclosure".

[i.45] DOD Cyber Crime Center (DC3): "DC3 and DCSA Partner to Announce Vulnerability Disclosure Program for Defense Industrial Base".

[i.46] FIRST: "2024 Q3 Vulnerability Forecast".

[i.47] FIRST: "Cyber Insurance SIG".

[i.48] Center for Internet Security: "Reasonable Cybersecurity Guide".

[i.49] ISO/IEC TR 5895: "Cybersecurity -- Multi-party coordinated vulnerability disclosure and handling".

[i.50] ISO/IEC 29147: "Information technology -- Security techniques -- Vulnerability Disclosure".

[i.51] OASIS Common Security Advisory Framework (CSAF) TC.

[i.52] Recommendation ITU-T X.1520: "Common vulnerabilities and exposures".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

BLACKER: end-to-end encryption system for computer data networks that was developed by NSA to provide host-to-host data confidentiality service for datagrams at OSI Layer 3

False Negatives (FN): incorrectly delayed vulnerabilities that were given a low EPSS score, but were found to be exploited in the observed data

False Positives (FP): incorrectly prioritized vulnerabilities with a high EPSS score, but were not exploited according to the observed data

patch Tuesday: practice by software vendors to accumulate security patches over a month, and dispatch them all on the second Tuesday of each month at a specific time to facilitate vulnerability remediation

rainbow series: set of NCSC computer security standards and guidelines published with coloured designations

True Negatives (TN): correctly delayed vulnerabilities that were given a low EPSS score, and were also not found to be exploited

True Positives (TP): correctly prioritized vulnerabilities with a high EPSS score, and were found to be exploited in the real world

vulnerability:

- security defect or bug in a system, product or service [i.9]
- flaw in a software, firmware, hardware, or service component resulting from a weakness that can be exploited, causing a negative impact to the confidentiality, integrity, or availability of an impacted component or components [i.11]
- functional behaviour of a product or service that violates an implicit or explicit security policy [i.12]
- weakness, susceptibility or flaw of ICT products or ICT services that can be exploited by a cyber threat [i.1]
- weakness in software, hardware, or a service that can be exploited [i.13]

- weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source [i.14]

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

EPSS	Exploit Prediction Scoring System
FIRST	Forum of Incident Response and Security Teams
FN	False Negatives
FP	False Positives
GSMA	GSM Association
NCSC	National Computer Security Center (US)
NCSC	National Computer Security Conference (US)
NCSC	National Cyber Security Centre (UK)
NSA	National Security Agency (US)
NTIA	National Telecommunication and Information Agency
SBOM	Software Bill Of Materials
TN	True Negatives
TP	True Positives

4 History

4.1 Timeline of cybersecurity vulnerability disclosure

The long historical arc of vulnerability disclosure across the past 230 years together with highlights described in subsequent clauses is depicted in Figure. 4.1-1.

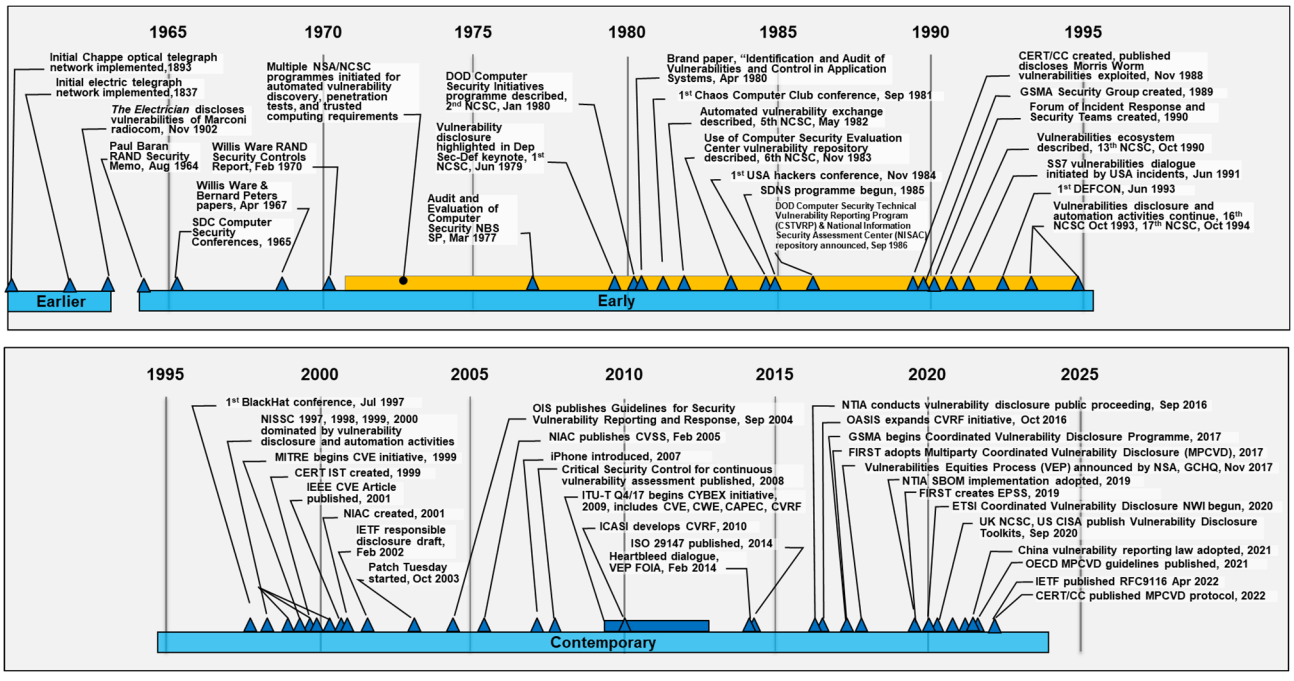


Figure 4.1-1: Vulnerability Disclosure Timeline

4.2 Origins

All communication networks and their diverse analogue and digital components and implementations have endemic and persistent vulnerabilities. The vulnerabilities are discovered, induced, manifested, and often exploited over time by an array of entities for both lawful and unlawful purposes that are all part of a complex and diverse ecosystem. Vulnerability disclosure in various forms, formats, and process are threaded through that ecosystem.

Excluding the existence of various forms of physical communication networks over the eons of human communication, the modern history of the vulnerability disclosure ecosystem dates back to the origins of France's optical telegraph networks in the 1790s which manifested the simple vulnerability of visual interception. The scale of the systems and vulnerabilities were significantly scaled 50 years later with the widespread emergence of electric telegraph networks, and then again at the beginning of the 20th century with the emergence of radiocommunication networks using the open "ether" for transport circuits.

The principal mitigation and exploit for the interception vulnerability of these early forms of communication consisted of cryptography, accounting, and physical security controls for the implementations.

4.3 Early period 1964 - 1995

Packet-switched data network technology emerged in the early 1960s based on the work of Paul Baran and Sharla Boehm at the RAND Corporation and Donald Davies at the UK National Physical Laboratory. Baran realized at the outset in 1964 that fundamental vulnerabilities existed in the use of the technology, see [i.38]. This reality led RAND two-years of NSA and RAND studies, and security scientists Bernard Peters and Willis Ware to assemble colleagues from their organizations at the 1967 AFIPS Spring Joint Computer Conference. The event followed two earlier conferences in 1965 hosted by the RAND spin-off, System Development Corporation (SDC), on safeguarding computer systems "operated in a time-shared mode." Ware was the founding president of American Federation of Information Processing Societies (AFIPS). His presentation at the conference together with eminent NSA computer scientist Bernard Peters - and especially the diagram on networked computer system vulnerabilities and associated risks (see Figure 4.3-1) - became the seminal and defining point for modern cybersecurity.

The companion conference paper by Peters - who subsequently developed the concepts and practices for penetration testing - focuses on security considerations in any "multi-programmed" computer system. An extraction from Peters' paper set forth what remain as the fundamentals of cybersecurity today:

"*1) security cannot be attained in the absolute sense;*

2) every security system seeks to attain a probability of loss which is commensurate with the value returned by the operation being secured;

3) for each activity, which exposes private, valuable, or classified information to possible loss, it is necessary that reasonable steps be taken to reduce the probability of loss;

4) any loss which might occur must be detected;

5) there are several minimum requirements to establish an adequate security level for the software of a [networked computer system;

6) management must be aware of the need for security safeguards and be willing to support the cost of obtaining this security protection;

7) it must be technically competent to judge whether or not a desired security level has been reached;

8) no software system can approach a zero risk of loss;

9) it is necessary to reach an acceptable degree of risk".

The two Atlantic City conference papers initiated a major responsive ARPA task force. Its report was assembled under the Defense Science Board and published as a 78 page US DOD 1970 report, *Security Controls for Computer Systems*, informally known as the "Ware Report." The Report identifies and extensively treats cybersecurity vulnerabilities, establishes an ontology, the strategic implications, and related processes - notably including vulnerability disclosure. The events here are widely held by computer security practitioners and historians to have defined the modern cybersecurity field's origin.

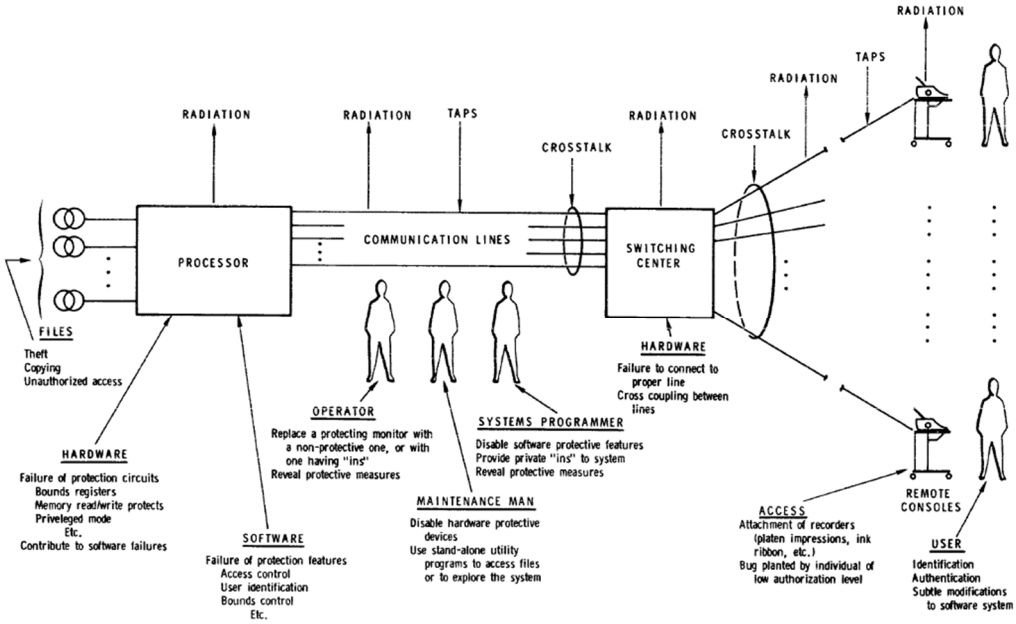


Figure 4.3-1: Networked computer system vulnerabilities and associated risks

During the subsequent two decades of the 1970s and 1980s, significant programmes ensued within the U.S. national security community that set the stage for cybersecurity vulnerability discovery, disclosure, mitigation, and information sharing. Many of these programmes resulted in automated discovery and cataloguing of vulnerabilities through penetration testing which endure as significant components of the vulnerability discovery ecosystem today. These initiatives include BLACKER, the Orange Book/Trusted Computer System Evaluation Criteria (TCSEC), and other documents of the Rainbow Series. The Bibliography provides references to source materials from this period, including a historical overview from the Babbage Institute which houses extensive personal collections from the leaders of the work.

Initially, the work was accomplished within the U.S. national security community. Some materials began to appear publicly in the late 1970s such as the National Bureau of Standards Special Publication on Audit and Evaluation of Computer Security that was constituted as proceedings from an invitational workshop in 1977. The security provisions included implementation plans based on analyses of the existing physical, technical, and administrative safeguards, and consideration of determinations by system managers of the vulnerabilities of their data and resources, and the protection necessary to safeguard against these vulnerabilities.

NSA's engagement with the public and vetting of major cybersecurity programs scaled significantly in June 1979 with the organization of the first of a twenty-year series of annual events known as the National Computer Security Conference (NCSC). The Assistant Secretary of Defence keynote address opening the first conference noted that "*there is always a potential for vulnerabilities with our hardware and software systems which we will have to protect by means of the physical and administrative measures that surround these systems*". The following year in April 1980 at the 2nd NCSC scaled to encompass a broad array of public and private sector computer security leaders and included a review of research and policy initiatives over the 1970-1980 period. The following year in 1980 saw the first NBS Special Publication focussed on vulnerability identification and auditing.

The year 1981 was marked by the appearance of what emerged as a significant and ever-expanding set of worlds in the vulnerability disclosure ecosystem - autonomous, private individuals and researchers with different motivations and incentives to discover vulnerabilities in networked computer systems. The 1st Chaos Computing Club (CCC) event was held in September 1981 at Berlin. The initial CCC participant motivations centred on capturing telephone network resources. The increasing use of remote computing access using packet data networks with an array of different internetworking arrangements, coupled with the release of the popular film *War Games* based on a real event involving teenage hackers, invented an expanding array of youth to partake in vulnerability discovery, exchange, and exploiting exercises; as well as an increasing level of concern by government and private industry security communities.

By the 5th NCSC in 1982, as the expansion of computer applications software expanded, focus began on automated application vulnerability discovery. At the 6th NCSC in late 1983, the implementation of the DOD Computer Security Evaluation Center vulnerability repository which was described. Meanwhile, the first USA hackers conference was held in November 1984 near San Francisco.

As the realization expanded in the 1980s within the U.S. national security community on the need for public telecommunication networks that reduced the expanding vulnerability knowledge base, the NSA embarked on a major public private programme to develop a Secure Data Network System (SDNS) to *"assist and encourage industry in developing a wide variety of INFOSEC products and systems to be made available in the marketplace at a cost and level of user friendliness to equally encourage widespread use of these products*". The SDNS programme begun in 1985 was announced at 10th NCSC in 1987. Meanwhile, the Computer Security Technical Vulnerability Reporting Program (CSTVRP) and National Information Security Assessment Center (NISAC) repository was announced in September 1986.

November 1988 was marked by two entwined notable events in the history of vulnerability disclosure. The creation and insertion of the Morris Worm into the infrastructure of DARPA's TCP/IP network caused the entire network to cease functioning and exposed multiple vulnerabilities. The event was the basis for DARPA's immediate creation of a permanent Computer Emergency Response Team (CERT) Coordination Center known as the CERT/CC at the Carnegie Mellon Software Engineering Institute. Thereafter, the CERT/CC became a model for similar activities in the private and public sector worldwide. In the years that followed, the processes, practices, and specifications established by the CERT/CC became the model for of much of subsequent activity in the vulnerability disclosure ecosystem and resulted in creation of the principal vulnerability disclosure international organization, FIRST (Forum of Incident Response and Security Teams) in 1990.

The year 1989 was also marked by the creation of the GSMA Security Group (SG) under the leadership of Charles Brookson. Over the subsequent decades, as the GSM global infrastructure became the principal means of telecommunication and personal computers migrated on to mobile devices connected to that infrastructure, SG would prove to principal means for effecting vulnerability disclosure and mitigations.

In the years that followed, hacker expertise, digital technologies, telecommunication deregulation and increasing exposure of public network interfaces results in vulnerability exploitation, significantly scaling incidents and threats. Notable events included a large-scale telephone network outage in 1991 and holding the first DEFCON conference in June 1993 that brought together a larger global vulnerability discovery community. Meanwhile, the US national security community described the vulnerabilities ecosystem at the 13th NCSC in 1990 and continued to report on related automation activities in 1993 and 1994. All of the events unfolding gave rise to vulnerability discovery and hacking in popular culture, captured in 1995 by publication of the best-selling book, CYBERPUNK: Outlaws and Hackers on the Computer Frontier by the New York Times reporters who broke Morris Worm story in 1988.

4.4 Contemporary period after 1995

After 1995, the vulnerability disclosure ecosystem was marked by never-ending scaling of the basic dimensions and tools already well-established as the actors, institutions, motivations, and challenges became increasingly complex and largely intractable. Bernard Peters original 1967 fundamentals became manifested ubiquitously.

The BlackHat conference began in 1997 and the U.S. national security NCSC conferences (which were re-named as the National Information Systems Security Conference (NISSC) after 1995) up to the last in 2000 became increasingly dominated by presentations on vulnerability disclosure and automation activities. The CCC, DEFCON, and BlackHat events subsequently constituted the most prominent and active events within the penetration testing and vulnerability detection communities and "bug economy" that emerged worldwide.

In response to these challenges, within the U.S. national security community, in the late 1990s, MITRE began pursuing what became the principle platforms and standards for structured capture, identification, evaluation, and exchange of vulnerability disclosures that eclipsed the work occurring within NSA and the CERT/CC over previous decades. The MITRE activity began with the Common Vulnerabilities and Exposures (CVE) standard in 1999 - which remains today the principal specification for expressing a cybersecurity vulnerability worldwide.

Over the following decade, the MITRE initiatives were amplified by the France CERT-IST which was also created in 1999, CVE knowledge conveyed via the IEEE™ in 2001, an IETF responsible disclosure draft published in 2002. The U.S. National Infrastructure Advisory Council was also created in 2001 to begin dealing with critical infrastructure vulnerabilities. The Organization for Internet Safety which for formed by several vendors in 2002 to coordinate vulnerability related activities, published guidelines for Security Vulnerability Report and Response in September 2004.

The pervasive existence of common highly complex operating systems with enormous code bases attackable via networks, led increasingly to vendors providing software patches which were necessary to eliminate the vulnerabilities. In October 2003, Microsoft introduced "Patch Tuesday" which provided an array of accumulated security patches at 12.00 Pacific Time on the second Tuesday of each month, and for which CVE notices were provided to the U.S. National Vulnerability database. However, the practice also produced an underground hacking economy where the patches were reverse engineered within 30 minutes, and vulnerability exploit were made available among hacking communities.

As the emergence of computer based mobile phones occurred with the iPhone announcement in 2007, the potential vulnerabilities of mobile devices increased significantly. With their integration into GSM networks globally and the ability to bypass secure access by using Wi-Fi®, the GSMA and its Security Group became the principal means for addressing those vulnerabilities. The complexities were underscored by the associated demands of Lawful Interception which necessitated the exploitation of vulnerabilities by government authorities while ensuring that judicial trust requirements were also met.

In 2005, NIAC published the most important adjunct to CVE, the Common Vulnerability Scoring System (CVSS), and subsequently transferred it to FIRST standards interest group to maintain and evolve. In 2008, the NSA Information Assurance Directorate (IAD), publicly advanced the Continuous Vulnerability Assessment Control as an essential component of the Critical Security Controls that is presently found in ETSI TR 103 305 [i.8]. The control provenance dates back to the 1967 AFIPS Atlantic City Conference presentation by Willis Ware and Bernard Peters.

As it had previously done in the 1980s, the U.S. began an array of cybersecurity initiatives in ITU-T SG17 beginning in 2007. In 2009, the U.S. assumed the chair of its Study Group 17 Cybersecurity standards group and comprehensive ensemble of standards known as the CYBEX initiative - including those encompassing vulnerability disclosure - were introduced and adopted. The CVE standard exists as Recommendation ITU-T X.1520 [i.52].

In 2010, the Common Vulnerability Reporting Framework (CVRF) standard was developed by the Industry Consortium for Advancement of Security on the Internet (ICASI), further evolved with the ITU-T CYBEX initiative, and ultimately pursued in OASIS as the principal structured specification for reporting vulnerabilities. In 2014, with the assistance of the CERT/CC, ISO/IEC 29147 [i.50] published its vulnerability disclosure guide,.

A highly public cybersecurity incident occurred that revealed a major vulnerability known as Heartbleed. A combination of national security leaks and litigation revealed the existence of the U.S. "Vulnerabilities Equities Process" or VEP. The U.S. government regulatory process is similar to those long existing in many countries where national security authorities seek to acquire knowledge of certain vulnerabilities to potentially further critical intelligence and defence interests, and a fundamental component of the vulnerability disclosure ecosystem.

From 2017 onwards, numerous organizations including GSMA, ETSI, UK NCSC, US CISA, IETF, and Australia ACSC, published vulnerability disclosure programmes and guides of different species [i.10], [i.18] and [i.23]. Two jurisdictions - China and the EU - published their requirements as law. Only one governmental entity - the US NTIA - created an advisory committee of participants in the vulnerability disclosure ecosystem and undertook a consultative proceeding to build a knowledge base, see [i.15]. Another significant vulnerability disclosure development is the creation of a FIRST Vulnerability Coordination SIG to develop a Multi-Party Coordinated Vulnerability Disclosure (MPCVD) specification [i.13].

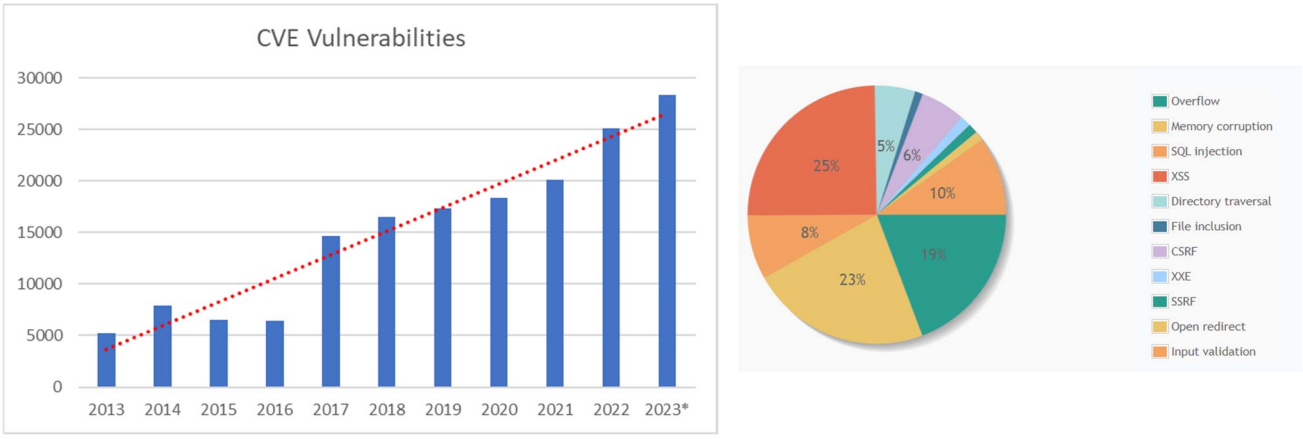
An OECD working party recommendation published in 2021 encouraged multi-party coordination and efficient identification of affected stakeholders as part of vulnerability treatment and responsible disclosure, see [i.30]. In 2022, the CERT/CC published a new protocol specification for Multi-Party Coordinated Vulnerability Disclosure (MPCVD) with the goal of improving the interoperability of both CVD and MPCVD process implementations, see [i.31]. Vultron is not a process compatibility protocol but an implementation compatibility protocol. It achieves this goal by formalizing the different steps of vulnerability disclosure, embargo management, exploit availability and so forth into a set of states. Each state is given a semantic definition. By agreeing on the semantic definition of key states, Vultron protocol participants (possibly on different platforms) can exchange information, synchronize and agree on the CVD / MPCVD next steps despite the possible divergence between their CVD process implementations and vulnerability handling process implementations. A CVD / MPCVD platform that implements Vultron can use the protocol, e.g. to assist the vulnerability handler in identifying the next possible steps.

In addition to programme expansions such as SBOM, other new derivative vulnerability platforms have emerged. For example, FIRST has further developed CVSS and created the Exploit Prediction Scoring System (EPSS), see [i.20]. CISA established a related system, Known Exploited Vulnerabilities (KEV), see [i.28]. Both platforms have automated integration capabilities. It should be noted that CVSS and EPSS are two separate tools that are used in a complementary fashion. To put it simply, CVSS deals with the characteristics of the vulnerCVSS and EPSS are two separate tools that are used in a complementary fashion. To put it simply, CVSS deals with the characteristics of the vulnerability, while EPPS attempts to evaluation the vulnerability risk through the lens of the exploitation "risk.ability", while EPPS attempts to evaluation the vulnerability risk through the lens of the exploitation risk.

4.5 Emerging trends: expansion of venues and activities

The inevitable exponential increase of potential vulnerabilities spread across an ever-expanding mesh of information networks, components, services, and underlying code over the past decade have resulted in an expanding array of damaging cyber incidents - both malicious and unintentional, see [i.17]. Increasingly, the incidents are attributable to nation-state attacks. These trends have resulted in increased actions being taken by government authorities and industry, including new capabilities, programmes, studies, and regulatory requirements related to vulnerability discovery. Additionally, it has produced a significantly expanded and evolving vulnerability disclosure marketplace and related sources of revenue known as the "bug economy", see [i.17] and [i.15]. Especially noteworthy is the resulting emergence of far-reaching Software Bill of Materials (SBOM) programmes, see [i.16], [i.29], [i.32], [i.33] and [i.34].

In many ways, however, the ecosystem itself described in clause 5 below has remained the same since the challenges were first identified publicly in 1967. Sets of sources discover vulnerabilities which are identified in repositories. Some vulnerabilities are retained by national security authorities. Generally, software patches or remediations for those vulnerabilities are provided to system administrators end users to prevent or alleviate cybersecurity incidents and exploitations. What has changed are the scale, complexity and dynamics which make integration and automation of vulnerability disclosures critical. Figure 4.5-1 depicts the growth and trend line of vulnerabilities published by the most commonly referenced source, the U.S. National Vulnerability Database (NVD), as well as the relative percentages of vulnerability types. Figure 4.5-2 depicts the relative percentages of seriousness of the vulnerabilities based on CVSS scores - with the preponderance being in the higher categories.



NOTE: Projected from Jan-Jul 2023.

Figure 4.5-1: CVE reported vulnerabilities trend and types (Source: [i.19])

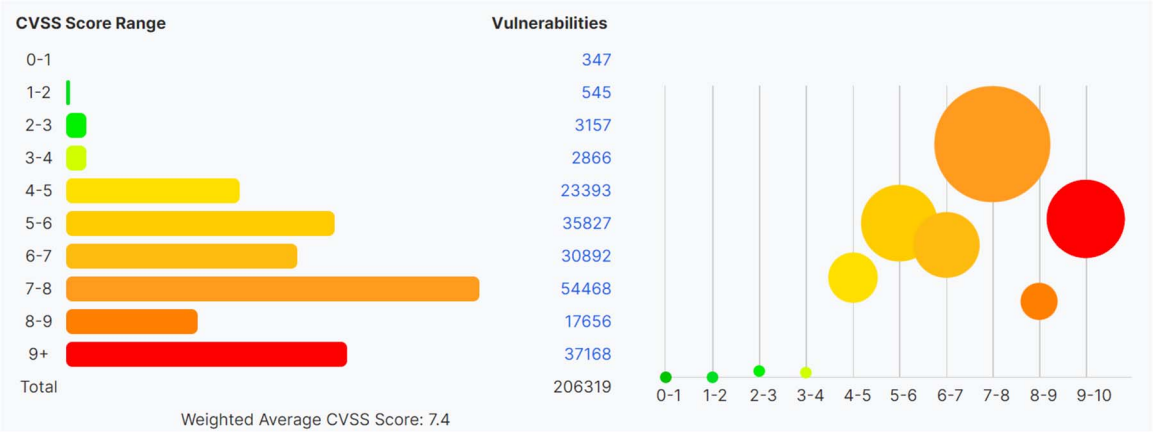


Figure 4.5-2: Distribution of vulnerabilities by CVSS scores (Source: [i.19])

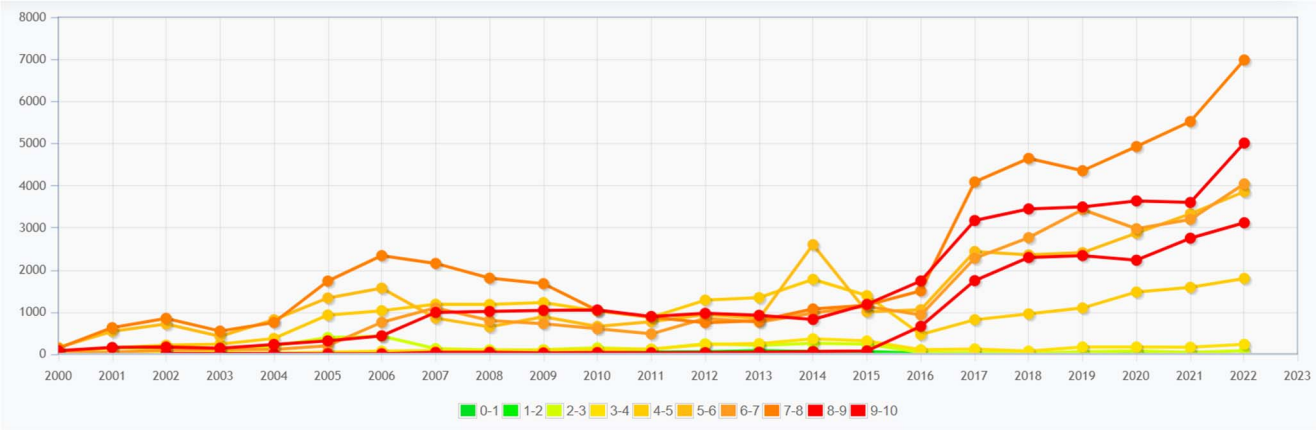


Figure 4.5-3: CVE reported vulnerabilities trend by CVSS scores (Source: [i.19])

Figure 4.5-3 depicts the trend lines over time for the vulnerabilities depicted in Figure 5.1-1, showing that from 2016 onwards, the more serious vulnerabilities have significantly increased.

As Wikipedia's extensive discussion of the vulnerability marketplace notes, "exploits are digital products, which means that they are information goods with near-zero marginal production costs", see [i.21]. Once they are exposed, however, the value decreases significantly, but does not go to zero because patch implementations are asymmetric, knowledge of the details has a value to those developing exploits. The result is a kind of black-market cyber-arms industry. On average, zero-day vulnerabilities have a value between $10,000 and $100,000. From a public policy perspective, however, knowledge of vulnerabilities in public databases does not appear to have value in predicting other vulnerabilities, see [i.22].

The two largest of the vulnerability discovery and penetration testing tradeshows - Blackhat and DEFCON - have grown significant in recent years in attendance, vendors, and globalization. Both the USA Blackhat and DEFCON events in Las Vegas in 2022 drew more than 21,000 people from 111 countries and nearly 400 exhibitors, with smaller events in Europe, Middle East, and Asia. Both government agencies and private sector companies in the vulnerability disclosure ecosystem significantly engage in these events for both intelligence and prospective employees.

ENISA's 2018 Report prepared with the assistance of the RAND Corporation on the economics of the revealed a steady expansion of the "vulnerability marketplace". The Report portrayed an array of marketplace actors and the global "bug bounty" platforms market was valued at $1.13 billion in 2022 and expected to grow at a 16 % CAGR in the coming years, see [i.17]. The Report also noted that "governments are multifaceted actors in the vulnerability disclosure process and may perform several roles, including the role of finder, vendor/vulnerability owner, vulnerability coordinator, or those responsible for vulnerability stockpiling." "The study findings also emphasize the importance of approaching vulnerability disclosure as an ecosystem." Legislation was also significantly treated, noting "legislation that clearly outlines what is legally admissible to do as part of a vulnerability identification process may put security researchers at ease, allowing them to undertake vulnerability finding activities without risking legal action in contrast, overly restrictive or misaligned legislation may, in turn, have chilling effects on vulnerability disclosure and result in fewer security researchers engaging in vulnerability identification and disclosure" [i.17].

The USA NTIA advisory committee for "Multistakeholder Process To Promote Collaboration on Vulnerability Research Disclosure" referenced the ENISA Report and underscored the complexities and the potential adverse consequences of legislative/regulatory interventions, see [i.15]. The result of these reports and similar activities in most jurisdictions has led to national authorities to encourage widespread organizational development and publication of vulnerability disclosure policies, also known as Coordinated Vulnerability Disclosure, see [i.25]. Although the published policies are now ubiquitous, it has also led to the collateral consequence of expanding what is sometimes called "the fog of more", see [i.24].

The general lack of direct utility of vulnerability disclosure policies combined with the "fog of more" vulnerabilities have had several major consequences. The collateral emergence of Software Bill of Materials (SBOM) programmes attempt facilitate discovery and mitigation of vulnerabilities as part of supply chains, see [i.16]. It has also enormously expanded the markets for vulnerability aggregators and evaluators as a service together with the integration of that information into automated cybersecurity control mechanisms. Critical Security Control 4 is Continuous Vulnerability Assessment and Remediation that follows from the first three Controls that encompass device and software inventories and knowledge of their configurations, see [i.8].

Perhaps the most recent emerging trends related to vulnerability disclosure concern network virtualisation and Artificial Intelligence technologies, together with the place of vulnerability disclosure in the Zero Trust Model (ZTM) with continuous monitoring. The ZTM assumes that vulnerabilities are pervasive and mitigations intractable - placing the emphasis instead on continuous monitoring of network object behaviour at necessary points in the network, see [i.26] and [i.27].

Two regulatory jurisdictions - China and the EU have recently pursued the enactment of vulnerability disclosure regulatory mandates with significant penalties for non-compliance, see [i.1], [i.2], [i.3], [i.4] and [i.5]. The most far reaching is the EU Cyber Resiliency Act. Both the China and the EU "regulate the discovery, reporting, patching, and release of network product security vulnerabilities, and to prevent network security risks" [i.5]. The domestic and extraterritorial effects on the vulnerability disclosure ecosystem remain unknown, as there are no conflict of law provisions in the enactments.

Restructuring and enriching the National Vulnerability Database

One of the most significant changes in the vulnerability disclosure ecosystem began to unfold in 2024 along several paths. NIST cessation of analytical data additions to the NVD caused automated tools to be less effective that emerged from a significant increase in vulnerabilities between 2022 and 2023, see [i.40]. This cessation in turn resulted in the creation of new "open-source" NVDs, see [i.41]. In addition, CISA via MITRE, created a new CVE Program Mission to add NVD enrichment capabilities, see [i.42] and [i.43]. The enrichment includes stakeholder-specific vulnerability categorization (SSVC) decision points, CWE identifiers, CPE strings, CVSS calculations, and KEV flags. See clause 5.2.4.

5 Vulnerability disclosure ecosystem

5.1 Vulnerability disclosure marketplace

As concluded in the ENISA report on the vulnerability economics, the vulnerability disclosure ecosystem is best treated as a marketplace, see [i.17]. That marketplace structure and the participants have remained very stable over the decades and is depicted in Figure 5.1-1.

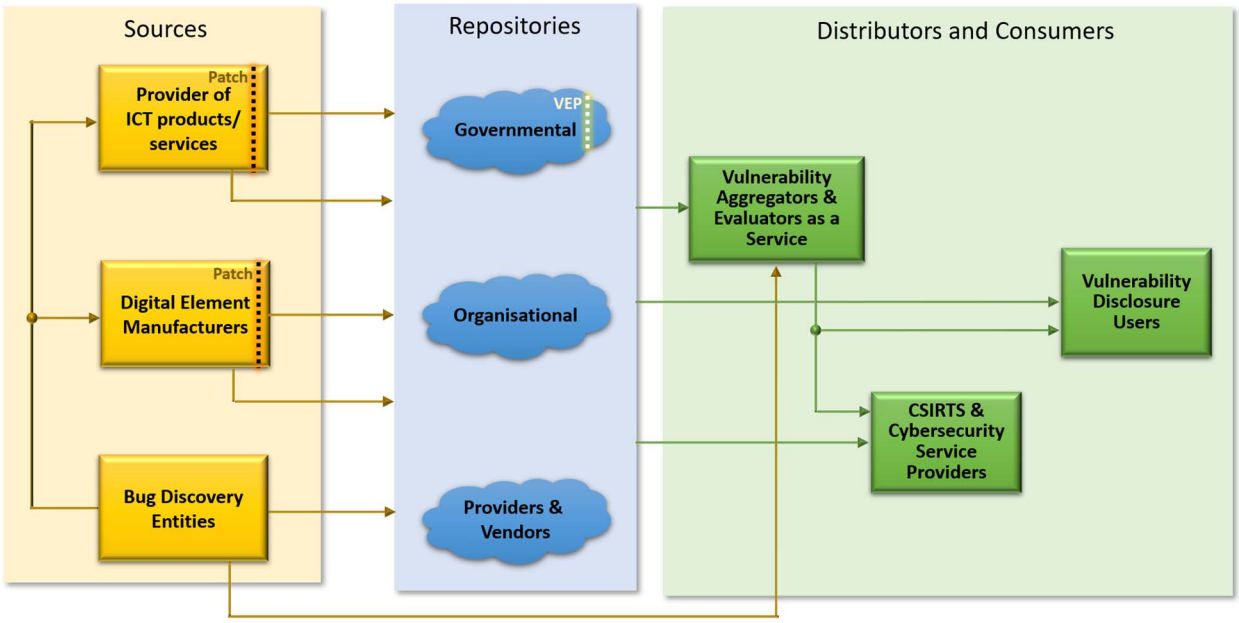


Figure 5.1-1: Vulnerability Disclosure Marketplace

5.2 Vulnerability Disclosure Ecosystem Ontology

5.2.1 Sources

Vast arrays of vulnerability sources have emerged that include product vendors, government agencies, CSIRTS, bug bounty providers, and hacker conferences - often referred to as "finders".

It is essential for product vendors to distribute patches prior to public vulnerability announcements. Vulnerability announcements introduce large-scale threats and potential attacks until patches are universally implemented.

Source information is frequently unstructured, unverifiable, and redundant.

5.2.2 Repositories

A number government, sector/organizational, and provider/vendor vulnerability repositories now exist. Figure 5.2.2-1, below lists well-known repositories. Sharing among the repositories is opaque. Provenance and value of repository vulnerability information may be problematic. These variances in turn have created secondary markets for diverse third-party analytical distributors who curate the repository information and tailor it for customers.

Name/URI	Format/Identifiers
Common Vulnerabilities and Exposures (CVE)	CVE+"enrichment"
NVD-Data-Overrides	CVE5+
Known Exploited Vulnerability Catalog (KEV)	CSV+JSON
VulDB	CVE, VDB
Mend Vulnerability Database	CVE, WS, MSC
CN National Vulnerability Database (CNNVD)	CVE, CNCVD
China National Vulnerability Database (CNVD)	CVE, CNVD
European Vulnerability Database (EUVDB) [i.44]	CVE

Figure 5.2.2-1: Well-Known Vulnerability Repositories

The need for improvements to vulnerability repositories has led the Cloud Security Alliance to create a working group, the Global Security Database (GSD), see [i.35]. Other related initiatives to deal with the deficiencies of existing reporting and identification of vulnerabilities include those of the open source and IoT communities, see [i.36] and [i.37].

5.2.3 Distributors

Vulnerability evaluators and distributors - frequently with automated tool interfaces - have grown in the marketplace and become essential. Vulnerability Exploitability eXchange (VEX) indicates the status of a software product or component with respect to a vulnerability, and integrates with SBOM, vulnerability databases, and security advisories together with CycloneDX.

5.2.4 Vulnerability discovery tools and sharing protocols

One of most significant advances vulnerability sharing protocol is the emergence of EPSS at FIRST - the Exploit Prediction Scoring System. EPSS is an open community-driven effort to model and manage vulnerability risk from a probabilistic perspective. EPSS takes data from multiple sources ranging from vendor reports to data published by researchers and white hat hackers, then categorizes vulnerabilities as False Positives (FP), True Positives (TP), False Negatives (FN), and True Negatives (TN). EPSS aims to measure mathematically the efficiency and the proportion of exploited vulnerabilities that were covered by the EPSS model. An EPSS model uses all available knowledge of vulnerabilities in the cybersecurity community, and then devise risk tolerance levels and vulnerability management activities based on scores that deliver the best efficiency and highest coverage, see [i.20].

Another significant vulnerability discovery and sharing tool is the CISA Known Exploited Vulnerabilities (KEV) online, continuously updated catalogue established in 2021, see [i.28]. KEV exists in multiple structured language formats and includes patch information. KEV facilitates use of vulnerability management frameworks - such as the Stakeholder-Specific Vulnerability Categorization (SSVC) model which consider a vulnerability's exploitation status. Organizations should also consider using automated vulnerability and patch management tools that automatically incorporate and flag or prioritize KEV vulnerabilities.

The Stakeholder-specific Vulnerability Categorization (SSVC) is a system for prioritizing actions during vulnerability management. SSVC aims to avoid one-size-fits-all solutions in favour of a modular decision-making system with clearly defined and tested parts that vulnerability managers can select and use as appropriate to their context, see [i.39]. SSVC takes the form of decision trees and that avoids some problems with the Common Vulnerability Scoring System (CVSS).

Vulnerability discovery and sharing protocols are rapidly evolving under new programs undertaken by CISA, MITRE, FIRST, OASIS, and the Open Source community to enrich and automate the activities, see [i.41], [i.42], [i.43], and [i.51].

5.2.5 Obligation requirements

5.2.5.1 Legislative and regulatory mandates

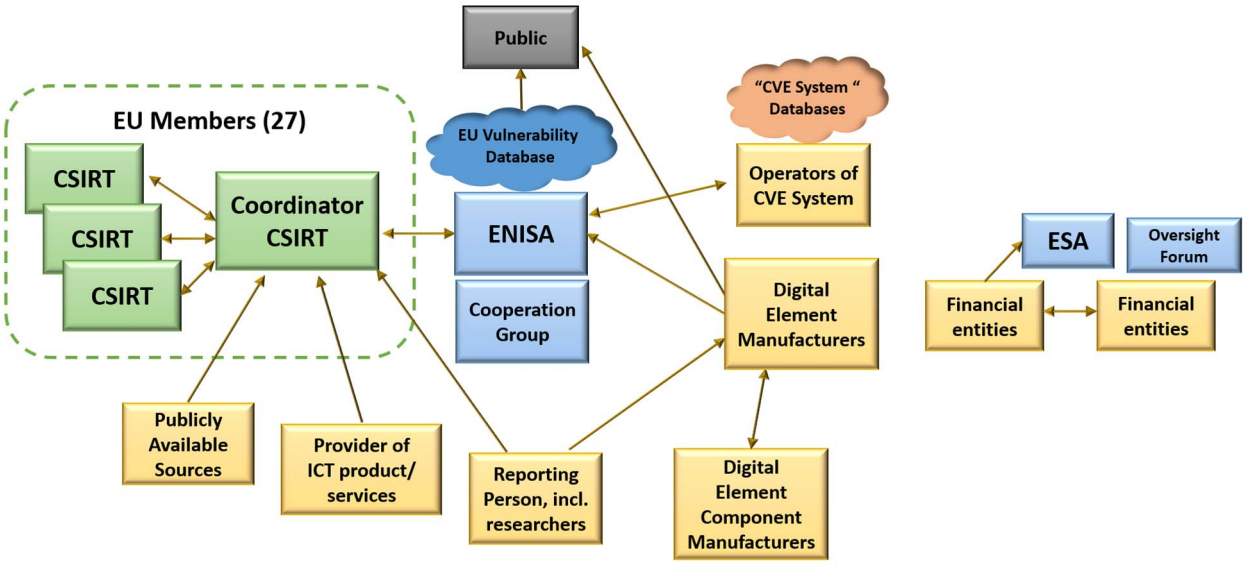


Figure 5.2.5.1-1: EU Vulnerability Disclosure Regulations

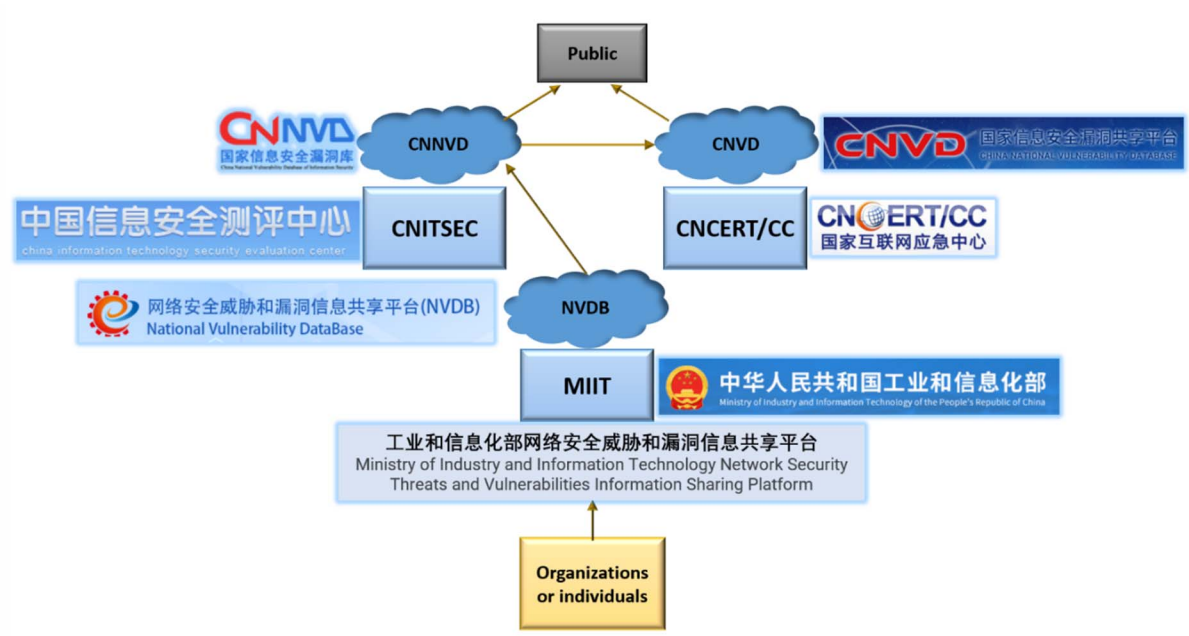


Figure 5.2.5.1-2: China Vulnerability Disclosure Regulations

5.2.5.2 Compulsory National Security practices

Almost every nation with an established national security agency maintains a Vulnerabilities Equities Process (VEP) obligation. VEP is a process used the agency to determine on a case-by-case basis how it should treat zero-day computer security vulnerabilities: whether to disclose them to the public to help improve general computer security, or to keep them secret for intelligence or law enforcement use, see [i.5], [i.6] and [i.7].

5.2.5.3 Contractual requirements (especially government clients)

Contracts between suppliers of products or services and their customers also establish vulnerability disclosure obligations. Such obligations are established both by industry Groups such as GSMA and the US Defense Industrial Base, see [i.12] and [i.45].

5.2.5.4 Insurance requirements

Increasingly, cyber insurance and reinsurance organizations are joining with the vulnerability standards community to establish the related obligations. Insurance produces a de facto standard through requirements during the process of offering insurance (underwriting). In order to establish and maintain essential cyber security across businesses, it is essential to maintain continuous feedback mechanism between CERTs and insurers/reinsurers. Specifications include sources of data for cyber insurers, actuaries, cyber risk modelers, CERTs, and digital forensics and incident response organizations [i.47]. The objective is to promote a more statistical and scientific approach to cyber risk and provide advice on the interpretation and limitations of such data, see [i.46].

5.2.5.5 Judicial decisions

In recent years, cybersecurity negligence claims under both statutory and common law have proliferated in many countries and given rise to the insurance requirements described in the above clause. Continuous vulnerability assessment is one of several important defences to causes of action brought against a provider to demonstrate reasonable cybersecurity measures, see [i.48].

6 Challenges

The rapidly evolving vulnerability disclosure ecosystem has created significant gaps on multiple planes. One gap plane exists among vendors and their ability to effectively discover and remediate vulnerabilities. Another gap plane is among regulators and their inability to comprehend the ecosystem, or recognize that vulnerabilities cannot be eliminated, and promulgate mandates that are impossible to implement and exacerbate threats arising from threats they create. Another gap plane exists within the diverse technical communities engaged in vulnerability disclosure activities and understanding the new vulnerability discovery and sharing tools becoming available.

The FIRST vulnerability forecasts provide insight into a seemingly unchanging constant - that vulnerabilities will continue to increase at what currently appears to be an increasing pace.

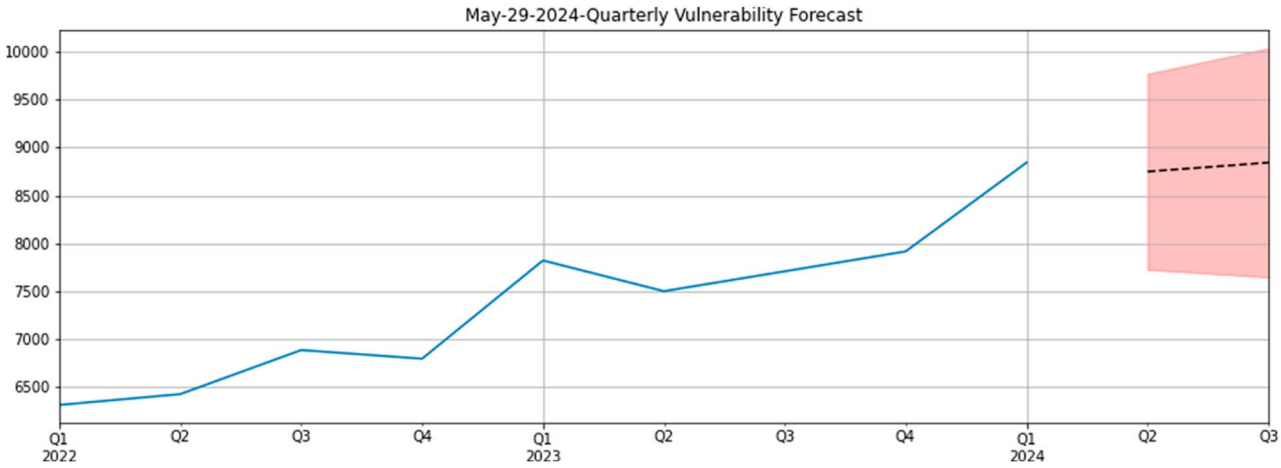


Figure 6-1: FIRST 29 May 2024 Quarterly Vulnerability Forecast (Source: [i.46])

The vulnerability disclosure challenges are numerous and constantly evolving. The enumeration of challenges below is not intended to be exhaustive - only representative of those present in the ecosystem:

- **Multi-Party Coordinated Vulnerability Disclosure:** The constantly growing complexity of physical product and software assembly and supply chains has increased the number and types of participants that participate in CVD. This is supported by guidelines such as those from FIRST [i.13] and ISO [i.49] that complement international standards on vulnerability disclosure and handling, see [i.50]. However, implementation of MPCVD represents a significant operational challenge to any organization.

- **Repository discovery:** Repositories of vulnerability information have proliferated. They are all inherently incomplete. There is no global mechanism for their discovery. This challenge has been exacerbated by recent regulatory requirements that mandate still more repositories with limited value proposition - often in different formats.

- **Assessment of vulnerability information:** The detail and quality of assessments remains challenging and incomplete. The recent efforts to "enrich" the information is critical to effective and timely use of the information.

- **Timing of public information:** The disclosure of vulnerability to the public or even within relatively closed communities can give rise to significant cybersecurity threats. Disclosed vulnerability information of any significance has significant economic value and typically is reverse engineered for exploitation and made available by cyber criminals in less than an hour. The development of software patches and their implementation in large infrastructures or among the dispersed public is complex and time consuming. Recent legislative mandates on public disclosure are themselves significant vulnerabilities.

- **Prohibitions against vulnerability discovery or vulnerability information distributors:** In some national jurisdictions, the discovery of vulnerabilities by third parties is criminalised, as is the distribution of that information among third parties. Because vulnerability discovery in the "bug economy" is largely driven by third parties, such prohibitions are extremely counter-productive.

- **Effective vulnerability disclosure mechanisms for AI, NFV and other dynamic platforms:** The introduction on a large scale of AI, NFV and other dynamic system and software platforms exacerbates the ability to discover and remediate vulnerabilities. Recent efforts to "enrich" vulnerability expressions and facilitate the use of automated tools should assist in implementing remediations.

- **Standards not effectively accessible:** Placing any vulnerability related standards or normative specifications behind paywalls is not only counterproductive, but as recently recognized by the European Court of Justice, a human rights impairment.

- **Special challenges of SMEs and general public:** The resources necessary for SMEs and the general public to understand the complexities of vulnerability disclosure and effect meaningful remediations is a significant barrier to mitigating the potential threats presented.

Annex A: Bibliography

- CISA: "Vulnerability-Exploitability eXchange (VEX) - An Overview", September 2021.
- CISA: "Vulnerability Exploitability eXchange (VEX) - Use Cases", April 2022.
- NTIA: "Multistakeholder Process: Cybersecurity Vulnerabilities".
- NTIA: "NTIA Software Component Transparency", April 2021.
- NTIA: "Software Bill of Materials".
- IEEE Spectrum: "What the Count of Monte Cristo Can Teach Us About Cybersecurity".
- Flashpoint: "Marconi's Wireless Telegraph and the First Vulnerability".
- David Kahn: "The Code-Breakers: The Story of Secret Writing".
- Misa, IEEE™ Annals of the History of Computing: "Computer Security Discourse at RAND, SDC, and NSA (1958-1970)".
- System Development Corporation: "Security in the Computer Environment".
- An Interview with Marvin Schaefer on 20 November 2013: "Computer Security History Project".
- Willis Ware, AFIPS Conference Proceedings, Atlantic City, 1967, at 279: "Security and privacy in computer systems".
- Bernard Peters, AFIPS Conference Proceedings, Atlantic City, 1967 at 283: "Security Considerations in a multi-programmed computer system".
- U.S. DOD: "Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security", 11 February 1970 (Ware Report).
- Murdoch, Bond & Anderson: "How Certification Systems Fail: Lessons from the Ware Report," How Certification Systems Fail: Lessons from the Ware Report".
- INFOSEC Institute: "The history of penetration testing".
- US DOD: "Handbook for the Computer Security Certification of Trusted Systems".
- NSA/NCSC Rainbow Series.
- NBS Special Publication 500-19: "Computer Science & Technology: Audit and Evaluation of Computer Security", Proceedings of the NBS Invitational Workshop held at Miami Beach, Florida, March 22-24, 1977.
- NBS Special Publication 500-95: "Audit and Evaluation of Computer Security II: System Vulnerabilities and Controls".
- Drautreporter: "Die Geschichte des Chaos Computer Clubs: Datendämmerung".
- Wikipedia: "The Hackers Conference".
- Tater & Kerut: "The Secure Data Network System: an overview", in Proceedings of the 10th National Computer Security Conference, 21-24 September 1987.
- UK NCSC: "Vulnerability Disclosure Toolkit".
- Center for Strategic and International Studies: "Significant Cyber Incidents", June 2023.
- Microsoft®: "Microsoft Digital Defense Report 2022".
- Google® Project Zero, Vulnerability Disclosure FAQ.

- IoT Security Foundation: "Vulnerability Disclosure", Release 2.0, 2021.
- IoT Security Foundation: "The Contemporary Use of Vulnerability Disclosure in IoT", Report 4: November 2021.
- RAND: "To Disclose, or Not to Disclose, That Is the Question".
- ENISA: "Developing National Vulnerability Programmes: Challenges and initiatives".
- Splunk: "The Exploit Prediction Scoring System (EPSS) Explained".
- Computer Weekly: "Cyber experts urge EU to rethink vulnerability disclosure plans".
- Cyber: "A mixed response on EU's new vulnerability disclosure rules".
- Atlantic Council: "Dragon tails: Preserving international cybersecurity research".
- Jukka Ruohonen: "The Incoherency Risk in the EU's New Cyber Security Policies", 20 May 2024.

History

Document history		
V1.1.1	September 2024	Publication