**Vulnerability (computing)**

From Wikipedia, the free encyclopedia

Jump to: [navigation](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#mw-head), [search](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#p-search)

For other uses of the word "vulnerability", see [vulnerability](http://en.wikipedia.org/wiki/Vulnerability).

See also: [Vulnerability to malware](http://en.wikipedia.org/wiki/Malware#Vulnerability_to_malware), [Anti-malware strategies](http://en.wikipedia.org/wiki/Malware#Anti-malware_strategies), [CVE](http://en.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures), and [CVSS](http://en.wikipedia.org/wiki/CVSS)

In [computer security](http://en.wikipedia.org/wiki/Computer_security), a **vulnerability** is a weakness which allows an [attacker](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29) to reduce a system's [information assurance](http://en.wikipedia.org/wiki/Information_assurance).  
**Vulnerability** is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw.[[1]](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_note-1) To exploit a vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness. In this frame, vulnerability is also known as the [attack surface](http://en.wikipedia.org/wiki/Attack_surface).

[Vulnerability management](http://en.wikipedia.org/wiki/Vulnerability_management) is the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities"[[2]](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_note-2) This practice generally refers to [software vulnerabilities](http://en.wikipedia.org/wiki/Software_vulnerability) in computing systems.

A security risk may be classified as a vulnerability. The usage of vulnerability with the same meaning of risk can lead to confusion. The risk is tied to the potential of a significant loss. Then there are vulnerabilities without risk: for example when the affected [asset](http://en.wikipedia.org/wiki/Asset_%28computing%29) has no value. A vulnerability with one or more known instances of working and fully implemented attacks is classified as an exploitable vulnerability — a vulnerability for which an [exploit](http://en.wikipedia.org/wiki/Exploit_%28computer_security%29) exists. The **window of vulnerability** is the time from when the security hole was introduced or manifested in deployed software, to when access was removed, a security fix was available/deployed, or the attacker was disabled—see [zero-day attack](http://en.wikipedia.org/wiki/Zero-day_attack).

[Security bug](http://en.wikipedia.org/wiki/Security_bug) ([security defect](http://en.wikipedia.org/wiki/Malware#Security_defect)) is a narrower concept: there are vulnerabilities that are not related to software: hardware, site, personnel vulnerabilities are examples of vulnerabilities that are not software security bugs.

Constructs in [programming languages](http://en.wikipedia.org/wiki/Computer_language) that are difficult to use properly can be a large source of vulnerabilities.

|  |
| --- |
| **Contents**   * [1 Definitions](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#Definitions) * [2 Phenomenology](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#Phenomenology) * [3 Classification](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#Classification) * [4 Causes](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#Causes) * [5 Vulnerability consequences](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#Vulnerability_consequences) * [6 Vulnerability disclosure](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#Vulnerability_disclosure)   + [6.1 Vulnerability inventory](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#Vulnerability_inventory) * [7 Vulnerability disclosure date](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#Vulnerability_disclosure_date) * [8 Identifying and removing vulnerabilities](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#Identifying_and_removing_vulnerabilities) * [9 Examples of vulnerabilities](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#Examples_of_vulnerabilities)   + [9.1 Software vulnerabilities](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#Software_vulnerabilities) * [10 See also](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#See_also) * [11 References](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#References) * [12 External links](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#External_links) |

**Definitions**

[ISO](http://en.wikipedia.org/wiki/International_Organization_for_Standardization) [27005](http://en.wikipedia.org/wiki/ISO/IEC_27005) defines **vulnerability** as:[[3]](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_note-ISO27005-3)

*A weakness of an asset or group of assets that can be exploited by one or more threats*

where an *asset is anything that can has value to the organization, its business operations and their continuity, including information resources that support the organization's mission*[[4]](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_note-4)

[IETF](http://en.wikipedia.org/wiki/IETF) [RFC 2828](http://tools.ietf.org/html/rfc2828) define **vulnerability** as:[[5]](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_note-rfc2828-5)

*A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy*

The [Committee on National Security Systems](http://en.wikipedia.org/wiki/Committee_on_National_Security_Systems) of [United States of America](http://en.wikipedia.org/wiki/United_States) defined **vulnerability** in CNSS Instruction No. 4009 dated 26 April 2010 [National Information Assurance Glossary](http://en.wikipedia.org/wiki/National_Information_Assurance_Glossary):[[6]](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_note-CNSSI4009-6)

*Vulnerability — Weakness in an IS, system security procedures, internal controls, or implementation that could be exploited*

Many [NIST](http://en.wikipedia.org/wiki/NIST) publications define **vulnerability** in IT contest in different publications: FISMApedia [[7]](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_note-7) term [[8]](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_note-8) provide a list. Between them SP 800-30,[[9]](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_note-SP80030-9) give a broader one:

*A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.*

[ENISA](http://en.wikipedia.org/wiki/ENISA) defines **vulnerability** in [[10]](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_note-10) as:

*The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event [G.11] compromising the security of the computer system, network, application, or protocol involved.(ITSEC)*

[The Open Group](http://en.wikipedia.org/wiki/The_Open_Group) defines **vulnerability** in [[11]](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_note-11) as:

*The probability that threat capability exceeds the ability to resist the threat*.

[Factor Analysis of Information Risk](http://en.wikipedia.org/wiki/Factor_Analysis_of_Information_Risk) (FAIR) defines **vulnerability** as:[[12]](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_note-FAIR-12)

*The probability that an asset will be unable to resist the actions of a threat agent*

According FAIR vulnerability is related to Control Strength, i.e. the strength of a control as compared to a standard measure of force and the [threat](http://en.wikipedia.org/wiki/Threat_%28computer%29) Capabilities, i.e. the probable level of force that a threat agent is capable of applying against an asset.

[ISACA](http://en.wikipedia.org/wiki/ISACA) defines **vulnerability** in [Risk It](http://en.wikipedia.org/wiki/Risk_It) framework as:

*A weakness in design, implementation, operation or internal control*

Data and Computer Security: Dictionary of standards concepts and terms, authors Dennis Longley and Michael Shain, Stockton Press, [ISBN 0-935859-17-9](http://en.wikipedia.org/wiki/Special:BookSources/0935859179), defines **vulnerability** as:

*1) In computer security, a weakness in automated systems security procedures, administrative controls, Internet controls, etc., that could be exploited by a threat to gain unauthorized access to information or to disrupt critical processing. 2) In computer security, a weakness in the physical layout, organization, procedures, personnel, management, administration, hardware or softwarethat may be exploited to cause harm to the ADP system or activity. 3) In computer security, any weakness or flaw existing in a system. The attack or harmful event, or the opportunity available to a threat agent to mount that attack.*

Matt Bishop and Dave Bailey [[13]](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_note-13) give the following definition of computer **vulnerability**:

*A computer system is composed of states describing the current configuration of the entities that make up the computer system. The system computes through the application of state transitions that change the state of the system. All states reachable from a given initial state using a set of state transitions fall into the class of authorized or unauthorized, as defined by a security policy. In this paper, the definitions of these classes and transitions is considered axiomatic. A vulnerable state is an authorized state from which an unauthorized state can be reached using authorized state transitions. A compromised state is the state so reached. An attack is a sequence of authorized state transitions which end in a compromised state. By definition, an attack begins in a vulnerable state. A vulnerability is a characterization of a vulnerable state which distinguishes it from all non-vulnerable states. If generic, the vulnerability may characterize many vulnerable states; if specific, it may characterize only one...*

[National Information Assurance Training and Education Center](http://en.wikipedia.org/wiki/National_Information_Assurance_Training_and_Education_Center) defines **vulnerability**: [[14]](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_note-14)[[15]](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_note-15)

*A weakness in automated system security procedures, administrative controls, internal controls, and so forth, that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing. 2. A weakness in system security procedures, hardware design, internal controls, etc. , which could be exploited to gain unauthorized access to classified or sensitive information. 3. A weakness in the physical layout, organization, procedures, personnel, management, administration, hardware, or software that may be exploited to cause harm to the ADP system or activity. The presence of a vulnerability does not in itself cause harm; a vulnerability is merely a condition or set of conditions that may allow the ADP system or activity to be harmed by an attack. 4. An assertion primarily concerning entities of the internal environment (assets); we say that an asset (or class of assets) is vulnerable (in some way, possibly involving an agent or collection of agents); we write: V(i,e) where: e may be an empty set. 5. Susceptibility to various threats. 6. A set of properties of a specific internal entity that, in union with a set of properties of a specific external entity, implies a risk. 7. The characteristics of a system which cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment.*

**Phenomenology**

The term "vulnerability" relates to some other basic security terms as shown in the following diagram:[[5]](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_note-rfc2828-5)

+ - - - - - - - - - - - - + + - - - - + + - - - - - - - - - - -+

| An Attack: | |Counter- | | A System Resource: |

| i.e., A Threat Action | | measure | | Target of the Attack |

| +----------+ | | | | +-----------------+ |

| | Attacker |<==================||<========= | |

| | i.e., | Passive | | | | | Vulnerability | |

| | A Threat |<=================>||<========> | |

| | Agent | or Active | | | | +-------|||-------+ |

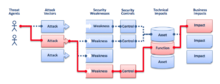
| +----------+ Attack | | | | VVV |

| | | | | Threat Consequences |

+ - - - - - - - - - - - - + + - - - - + + - - - - - - - - - - -+

A resource (either physical or logical) may have one or more vulnerabilities that can be exploited by a threat agent in a threat action. The result can potentially compromise the [confidentiality](http://en.wikipedia.org/wiki/Confidentiality), [integrity](http://en.wikipedia.org/wiki/Integrity) or [availability](http://en.wikipedia.org/wiki/Availability) of resources (not necessarily the vulnerable one) belonging to an organization and/or others parties involved(customers, suppliers).  
The so-called [CIA triad](http://en.wikipedia.org/wiki/CIA_triad) is the basis of [Information Security](http://en.wikipedia.org/wiki/Information_Security).

The attack can be *active* when it attempts to alter system resources or affect their operation: so it compromises integrity or availability. A "*passive attack*" attempts to learn or make use of information from the system but does not affect system resources: so it compromises Confidentiality.[[5]](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_note-rfc2828-5)

[](http://en.wikipedia.org/wiki/File:2010-T10-ArchitectureDiagram.png)

[http://bits.wikimedia.org/static-1.21wmf10/skins/common/images/magnify-clip.png](http://en.wikipedia.org/wiki/File:2010-T10-ArchitectureDiagram.png)

OWASP: relationship between threat agent and business impact

[OWASP](http://en.wikipedia.org/wiki/OWASP) (see figure) depicts the same phenomenon in slightly different terms: a threat agent through an attack vector exploits a weakness (vulnerability) of the system and the related security controls causing a technical impact on an IT resource (asset) connected to a business impact.

A set of policies concerned with information security management, the [information security management system](http://en.wikipedia.org/wiki/Information_security_management_system) (ISMS), has been developed to manage, according to [Risk management](http://en.wikipedia.org/wiki/Risk_management) principles, the [countermeasures](http://en.wikipedia.org/wiki/Countermeasure_%28computer%29) in order to accomplish to a security strategy set up following rules and regulations applicable in a country. Countermeasures are also called [Security controls](http://en.wikipedia.org/wiki/Security_controls); when applied to the transmission of information are named [security services](http://en.wikipedia.org/wiki/Security_service_%28telecommunication%29).[[16]](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_note-Vacca-16)

The overall picture represents the [risk factors](http://en.wikipedia.org/wiki/Risk_factor_%28computing%29) of the risk scenario.[[17]](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_note-17)

**Classification**

Vulnerabilities are classified according to the asset class they are related to:[[3]](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_note-ISO27005-3)

* hardware
  + susceptibility to humidity
  + susceptibility to dust
  + susceptibility to soiling
  + susceptibility to unprotected storage
* software
  + insufficient testing
  + lack of audit trail
* network
  + unprotected communication lines
  + insecure network architecture
* personnel
  + inadequate recruiting process
  + inadequate security awareness
* site
  + area subject to flood
  + unreliable power source
* organizational
  + lack of regular audits
  + lack of continuity plans
  + lack of security

**Causes**

* Complexity: Large, complex systems increase the probability of flaws and unintended access points [[18]](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_note-Vacca23-18)
* Familiarity: Using common, well-known code, software, operating systems, and/or hardware increases the probability an attacker has or can find the knowledge and tools to exploit the flaw [[19]](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_note-19)
* Connectivity: More physical connections, privileges, ports, protocols, and services and time each of those are accessible increase vulnerability [[12]](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_note-FAIR-12)
* Password management flaws: The computer user uses [weak passwords](http://en.wikipedia.org/wiki/Password_strength) that could be discovered by brute force. The computer user stores the password on the computer where a program can access it. Users re-use passwords between many programs and websites.[[18]](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_note-Vacca23-18)
* Fundamental [operating system](http://en.wikipedia.org/wiki/Operating_system) design flaws: The operating system designer chooses to enforce suboptimal policies on user/program management. For example operating systems with policies such as [default permit](http://en.wikipedia.org/wiki/Default_permit) grant every program and every user full access to the entire computer.[[18]](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_note-Vacca23-18) This operating system flaw allows viruses and malware to execute commands on behalf of the administrator. [[1]](http://www.ranum.com/security/computer_security/editorials/dumb/)
* Internet Website Browsing: Some internet websites may contain harmful [Spyware](http://en.wikipedia.org/wiki/Spyware) or [Adware](http://en.wikipedia.org/wiki/Adware) that can be installed automatically on the computer systems. After visiting those websites, the computer systems become infected and personal information will be collected and passed on to third party individuals.[[20]](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_note-20)
* [Software bugs](http://en.wikipedia.org/wiki/Software_bug): The programmer leaves an exploitable bug in a software program. The software bug may allow an attacker to misuse an application.[[18]](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_note-Vacca23-18)
* [Unchecked user input](http://en.wikipedia.org/wiki/Unchecked_user_input): The program assumes that all user input is safe. Programs that do not check user input can allow unintended direct execution of commands or SQL statements (known as [Buffer overflows](http://en.wikipedia.org/wiki/Buffer_overflow), [SQL injection](http://en.wikipedia.org/wiki/SQL_injection) or other non-validated inputs).[[18]](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_note-Vacca23-18)
* Not learning from past mistakes:[[21]](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_note-21)[[22]](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_note-22) for example most vulnerabilities discovered in [IPv4](http://en.wikipedia.org/wiki/IPv4) protocol software were discovered in the new [IPv6](http://en.wikipedia.org/wiki/IPv6) implementations [[23]](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_note-23)

The research has shown that the most vulnerable point in most information systems is the human user, operator, designer, or other human:[[24]](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_note-24) so humans should be considered in their different roles as asset, threat, information resources. [Social engineering](http://en.wikipedia.org/wiki/Social_engineering_%28security%29) is an increasing security concern.

**Vulnerability consequences**

|  |  |
| --- | --- |
| http://upload.wikimedia.org/wikipedia/en/thumb/9/99/Question_book-new.svg/50px-Question_book-new.svg.png | This section **needs additional citations for verification**. Please help [improve this article](http://en.wikipedia.org/w/index.php?title=Vulnerability_%28computing%29&action=edit) by [adding citations to reliable sources](http://en.wikipedia.org/wiki/Help:Introduction_to_referencing/1). Unsourced material may be [challenged](http://en.wikipedia.org/wiki/Template:Citation_needed) and [removed](http://en.wikipedia.org/wiki/Wikipedia:Verifiability#Burden_of_evidence). *(December 2010)* |

The impact of a security breach can be very high. The fact that IT managers, or upper management, can (easily) know that IT systems and applications have vulnerabilities and do not perform any action to manage the [IT risk](http://en.wikipedia.org/wiki/IT_risk) is seen as a misconduct in most legislations. [Privacy law](http://en.wikipedia.org/wiki/Privacy_law) forces managers to act to reduce the impact or likelihood that security risk. [Information technology security audit](http://en.wikipedia.org/wiki/Information_technology_security_audit) is a way to let other independent people certify that the IT environment is managed properly and lessen the responsibilities, at least having demonstrated the good faith. [Penetration test](http://en.wikipedia.org/wiki/Penetration_test) is a form of verification of the weakness and countermeasures adopted by an organization: a [White hat](http://en.wikipedia.org/wiki/White_hat) hacker tries to attack an organization information technology assets, to find out how is easy or difficult to compromise the IT security. [[25]](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_note-Vacca22-25) The proper way to professionally manage the IT risk is to adopt an [Information Security Management System](http://en.wikipedia.org/wiki/Information_Security_Management_System), such as [ISO/IEC 27002](http://en.wikipedia.org/wiki/ISO/IEC_27002) or [Risk IT](http://en.wikipedia.org/wiki/Risk_IT) and follow them, according to the security strategy set forth by the upper management. [[16]](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_note-Vacca-16)

One of the key concept of information security is the principle of [defence in depth](http://en.wikipedia.org/wiki/Defence_in_depth): i.e. to set up a multilayer defence system that can:

* prevent the exploit
* detect and intercept the attack
* find out the threat agents and prosecute them

[Intrusion detection system](http://en.wikipedia.org/wiki/Intrusion_detection_system) is an example of a class of systems used to detect [attacks](http://en.wikipedia.org/wiki/Attack_%28computing%29).

[Physical security](http://en.wikipedia.org/wiki/Physical_security) is a set of measures to protect physically the information asset: if somebody can get physical access to the information asset is quite easy to made resources unavailable to its legitimate users.

Some set of criteria to be satisfied by a computer, its operating system and applications in order to meet a good security level have been developed: [ITSEC](http://en.wikipedia.org/wiki/ITSEC) and [Common criteria](http://en.wikipedia.org/wiki/Common_criteria) are two examples.

**Vulnerability disclosure**

Responsible disclosure of vulnerabilities is a topic of great debate. As reported by The Tech Herald in August 2010, "[Google](http://en.wikipedia.org/wiki/Google), [Microsoft](http://en.wikipedia.org/wiki/Microsoft), [TippingPoint](http://en.wikipedia.org/wiki/TippingPoint), and [Rapid7](http://en.wikipedia.org/wiki/Rapid7) have recently issued guidelines and statements addressing how they will deal with disclosure going forward."[[26]](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_note-26)

A [responsible disclosure](http://en.wikipedia.org/wiki/Responsible_disclosure) first alerts the affected vendors confidentially before alerting [CERT](http://en.wikipedia.org/wiki/CERT_Coordination_Center) two weeks later, which grants the vendors another 45 day grace period before publishing a security advisory.

[full disclosure](http://en.wikipedia.org/wiki/Full_disclosure) is done when all the details of vulnerability is publicized, perhaps with the intent to put pressure on the software or procedure authors to find a fix urgently.

Well respected authors have published books on vulnerabilities and how to exploit them: [Hacking: The Art of Exploitation Second Edition](http://en.wikipedia.org/wiki/Hacking:_The_Art_of_Exploitation_Second_Edition) is a good example.

Security researchers catering to the needs of the [cyberwarfare](http://en.wikipedia.org/wiki/Cyberwarfare) or [cybercrime](http://en.wikipedia.org/wiki/Cybercrime) industry have stated that this approach does not provide them with adequate income for their efforts.[[27]](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_note-27) Instead, they offer their exploits privately to enable [Zero day attacks](http://en.wikipedia.org/wiki/Zero_day_attack).

The never ending effort to find new vulnerabilities and to fix them is called [Computer insecurity](http://en.wikipedia.org/wiki/Computer_insecurity).

**Vulnerability inventory**

[Mitre Corporation](http://en.wikipedia.org/wiki/Mitre_Corporation) maintains a list of disclosed vulnerabilities in a system called [Common Vulnerabilities and Exposures](http://en.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures), where vulnerability are classified (scored) using [Common Vulnerability Scoring System](http://en.wikipedia.org/wiki/CVSS) (CVSS).

OWASP collects a list of potential vulnerabilities in order to prevent system designers and programmers from inserting vulnerabilities into the software [[28]](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_note-28)

**Vulnerability disclosure date**

The time of disclosure of a vulnerability is defined differently in the security community and industry. It is most commonly referred to as "a kind of public disclosure of security information by a certain party". Usually, vulnerability information is discussed on a mailing list or published on a security web site and results in a security advisory afterward.

The **time of disclosure** is the first date a security vulnerability is described on a channel where the disclosed information on the vulnerability has to fulfill the following requirement:

* The information is freely available to the public
* The vulnerability information is published by a trusted and independent channel/source
* The vulnerability has undergone analysis by experts such that risk rating information is included upon disclosure

**Identifying and removing vulnerabilities**

Many software tools exist that can aid in the discovery (and sometimes removal) of vulnerabilities in a computer system. Though these tools can provide an auditor with a good overview of possible vulnerabilities present, they can not replace human judgment. Relying solely on scanners will yield false positives and a limited-scope view of the problems present in the system.

Vulnerabilities have been found in every major operating system[[*citation needed*](http://en.wikipedia.org/wiki/Wikipedia:Citation_needed)] including [Windows](http://en.wikipedia.org/wiki/Microsoft_Windows), [Mac OS](http://en.wikipedia.org/wiki/Mac_OS), various forms of [Unix](http://en.wikipedia.org/wiki/Unix) and [Linux](http://en.wikipedia.org/wiki/Linux), [OpenVMS](http://en.wikipedia.org/wiki/OpenVMS), and others. The only way to reduce the chance of a vulnerability being used against a system is through constant vigilance, including careful system maintenance (e.g. applying software patches), best practices in deployment (e.g. the use of [firewalls](http://en.wikipedia.org/wiki/Firewall_%28networking%29) and [access controls](http://en.wikipedia.org/wiki/Access_control)) and auditing (both during development and throughout the deployment lifecycle).

**Examples of vulnerabilities**

Vulnerabilities are related to:

* physical environment of the system
* the personnel
* management
* administration procedures and security measures within the organization
* business operation and service delivery
* hardware
* software
* communication equipment and facilities
* and their combinations.

It is evident that a pure technical approach cannot even protect physical assets: you should have administrative procedure to let maintenance personnel to enter the facilities and people with adequate knowledge of the procedures, motivated to follow it with proper care. see Social engineering (security).

Four examples of vulnerability exploits:

* an attacker finds and uses an overflow weakness to install malware to export sensitive data;
* an attacker convinces a user to open an email message with attached malware;
* an insider copies a hardened, encrypted program onto a thumb drive and cracks it at home;
* a flood damages your computer systems installed at ground floor.

**Software vulnerabilities**

Common types of software flaws that lead to vulnerabilities include:

* [Memory safety](http://en.wikipedia.org/wiki/Memory_safety) violations, such as:
  + [Buffer overflows](http://en.wikipedia.org/wiki/Buffer_overflow)
  + [Dangling pointers](http://en.wikipedia.org/wiki/Dangling_pointer)
* [Input validation](http://en.wikipedia.org/wiki/Data_validation) errors, such as:
  + [Format string attacks](http://en.wikipedia.org/wiki/Format_string_attack)
  + [SQL injection](http://en.wikipedia.org/wiki/SQL_injection)
  + [Code injection](http://en.wikipedia.org/wiki/Code_injection)
  + [E-mail injection](http://en.wikipedia.org/wiki/E-mail_injection)
  + [Directory traversal](http://en.wikipedia.org/wiki/Directory_traversal)
  + [Cross-site scripting](http://en.wikipedia.org/wiki/Cross-site_scripting) in web applications
  + [HTTP header injection](http://en.wikipedia.org/wiki/HTTP_header_injection)
  + [HTTP response splitting](http://en.wikipedia.org/wiki/HTTP_response_splitting)
* [Race conditions](http://en.wikipedia.org/wiki/Race_conditions), such as:
  + [Time-of-check-to-time-of-use](http://en.wikipedia.org/wiki/Time-of-check-to-time-of-use) bugs
  + [Symlink races](http://en.wikipedia.org/wiki/Symlink_race)
* [Privilege-confusion](http://en.wikipedia.org/wiki/Confused_deputy_problem) bugs, such as:
  + [Cross-site request forgery](http://en.wikipedia.org/wiki/Cross-site_request_forgery) in web applications
  + [Clickjacking](http://en.wikipedia.org/wiki/Clickjacking)
  + [FTP bounce attack](http://en.wikipedia.org/wiki/FTP_bounce_attack)
* [Privilege escalation](http://en.wikipedia.org/wiki/Privilege_escalation)
* [User interface](http://en.wikipedia.org/wiki/User_interface) failures, such as:
  + Warning fatigue [[2]](http://www.freedom-to-tinker.com/?p=459) or user conditioning [[3]](http://www.cs.auckland.ac.nz/%7Epgut001/pubs/phishing.pdf)
  + [Blaming the Victim](http://en.wikipedia.org/wiki/Victim_blaming) Prompting a user to make a security decision without giving the user enough information to answer it [[4]](http://blog.mozilla.com/rob-sayre/2007/09/28/blaming-the-victim/)
  + [Race Conditions](http://en.wikipedia.org/wiki/Race_Condition) [[5]](http://www.squarefree.com/2004/07/01/race-conditions-in-security-dialogs/) [[6]](http://lcamtuf.blogspot.com/2010/08/on-designing-uis-for-non-robots.html)

Some set of coding guidelines have been developed and a large [number of static code analysers](http://en.wikipedia.org/wiki/List_of_tools_for_static_code_analysis) has been used to verify that the code follows the guidelines.

**See also**

|  |  |
| --- | --- |
| [Portal icon](http://en.wikipedia.org/wiki/File:Monitor_padlock.svg) | [***Computer Security portal***](http://en.wikipedia.org/wiki/Portal:Computer_Security) |

* [Browser security](http://en.wikipedia.org/wiki/Browser_security)
* [Computer emergency response team](http://en.wikipedia.org/wiki/Computer_emergency_response_team)
* [Information security](http://en.wikipedia.org/wiki/Information_security)
* [Internet security](http://en.wikipedia.org/wiki/Internet_security)
* [Mobile security](http://en.wikipedia.org/wiki/Mobile_security)
* [Vulnerability scanner](http://en.wikipedia.org/wiki/Vulnerability_scanner)

**References**

* 1. [**^**](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_ref-1) ["The Three Tenents of Cyber Security"](http://www.spi.dod.mil/tenets.htm). U.S. Air Force Software Protection Initiative. Retrieved 2009-12-15.
  2. [**^**](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_ref-2) Foreman, P: *Vulnerability Management*, page 1. Taylor & Francis Group, 2010. [ISBN 978-1-4398-0150-5](http://en.wikipedia.org/wiki/Special:BookSources/9781439801505)
  3. ^ [***a***](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_ref-ISO27005_3-0) [***b***](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_ref-ISO27005_3-1) ISO/IEC, "Information technology -- Security tecniques-Information security risk management" ISO/IEC FIDIS 27005:2008
  4. [**^**](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_ref-4) British Standard Institute, Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management BS ISO/IEC 13335-1-2004
  5. ^ [***a***](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_ref-rfc2828_5-0) [***b***](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_ref-rfc2828_5-1) [***c***](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_ref-rfc2828_5-2) Internet Engineering Task Force [RFC 2828](http://tools.ietf.org/html/rfc2828) Internet Security Glossary
  6. [**^**](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_ref-CNSSI4009_6-0) [CNSS Instruction No. 4009](http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf) dated 26 April 2010
  7. [**^**](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_ref-7) [a wiki project](http://fismapedia.org/index.php) devoted to [FISMA](http://en.wikipedia.org/wiki/FISMA)
  8. [**^**](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_ref-8) [FISMApedia Vulnerability term](http://fismapedia.org/index.php?title=Term:Vulnerability)
  9. [**^**](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_ref-SP80030_9-0) [NIST SP 800-30 Risk Management Guide for Information Technology Systems](http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf)
  10. [**^**](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_ref-10) [Risk Management Glossary Vulnerability](http://www.enisa.europa.eu/act/rm/cr/risk-management-inventory/glossary#G52)
  11. [**^**](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_ref-11) Technical Standard Risk Taxonomy [ISBN 1-931624-77-1](http://en.wikipedia.org/wiki/Special:BookSources/1931624771) Document Number: C081 Published by The Open Group, January 2009.
  12. ^ [***a***](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_ref-FAIR_12-0) [***b***](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_ref-FAIR_12-1) ["An Introduction to Factor Analysis of Information Risk (FAIR)", Risk Management Insight LLC, November 2006](http://www.riskmanagementinsight.com/media/docs/FAIR_introduction.pdf);
  13. [**^**](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_ref-13) Matt Bishop and Dave Bailey. A Critical Analysis of Vulnerability Taxonomies. Technical Report CSE-96-11, Department of Computer Science at the University of California at Davis, September 1996
  14. [**^**](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_ref-14) Schou, Corey (1996). Handbook of INFOSEC Terms, Version 2.0. CD-ROM (Idaho State University & Information Systems Security Organization)
  15. [**^**](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_ref-15) [NIATEC Glossary](http://niatec.info/Glossary.aspx?term=6018&alpha=V)
  16. ^ [***a***](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_ref-Vacca_16-0) [***b***](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_ref-Vacca_16-1) Wright, Joe; Jim Harmening (2009) "15" *Computer and Information Security Handbook* Morgan Kaufmann Publications Elsevier Inc p. 257 [ISBN](http://en.wikipedia.org/wiki/International_Standard_Book_Number) [978-0-12-374354-1](http://en.wikipedia.org/wiki/Special:BookSources/978-0-12-374354-1)
  17. [**^**](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_ref-17) [ISACA THE RISK IT FRAMEWORK (registration required)](http://www.isaca.org/Knowledge-Center/Research/Documents/RiskIT-FW-18Nov09-Research.pdf)
  18. ^ [***a***](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_ref-Vacca23_18-0) [***b***](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_ref-Vacca23_18-1) [***c***](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_ref-Vacca23_18-2) [***d***](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_ref-Vacca23_18-3) [***e***](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_ref-Vacca23_18-4) Kakareka, Almantas (2009) "23" *Computer and Information Security Handbook* Morgan Kaufmann Publications Elsevier Inc p. 393 [ISBN](http://en.wikipedia.org/wiki/International_Standard_Book_Number) [978-0-12-374354-1](http://en.wikipedia.org/wiki/Special:BookSources/978-0-12-374354-1)
  19. [**^**](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_ref-19) [Technical Report CSD-TR-97-026 Ivan Krsul The COAST Laboratory Department of Computer Sciences, Purdue University, April 15, 1997](http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.26.5435&rep=rep1&type=pdf)
  20. [**^**](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_ref-20) [The Web Application Security Consortium Project, Web Application Security Statistics 2009](http://projects.webappsec.org/w/page/13246989/Web-Application-Security-Statistics#APPENDIX2ADDITIONALVULNERABILITYCLASSIFICATION)
  21. [**^**](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_ref-21) Ross Anderson. Why Cryptosystems Fail. Technical report, University Computer Laboratory, Cam- bridge, January 1994.
  22. [**^**](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_ref-22) Neil Schlager. When Technology Fails: Signi cant Technological Disasters, Accidents, and Failures of the Twentieth Century. Gale Research Inc., 1994.
  23. [**^**](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_ref-23) [Hacking: The Art of Exploitation Second Edition](http://en.wikipedia.org/wiki/Hacking:_The_Art_of_Exploitation_Second_Edition)
  24. [**^**](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_ref-24) Kiountouzis, E. A.; Kokolakis, S. A. *Information systems security: facing the information society of the 21st century* London: [Chapman & Hall](http://en.wikipedia.org/wiki/Chapman_%26_Hall), Ltd [ISBN](http://en.wikipedia.org/wiki/International_Standard_Book_Number) [0-412-78120-4](http://en.wikipedia.org/wiki/Special:BookSources/0-412-78120-4)
  25. [**^**](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_ref-Vacca22_25-0) Bavisi, Sanjay (2009) "22" *Computer and Information Security Handbook* Morgan Kaufmann Publications Elsevier Inc p. 375 [ISBN](http://en.wikipedia.org/wiki/International_Standard_Book_Number) [978-0-12-374354-1](http://en.wikipedia.org/wiki/Special:BookSources/978-0-12-374354-1)
  26. [**^**](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_ref-26) [The Tech Herald: The new era of vulnerability disclosure — a brief chat with](http://www.thetechherald.com/article.php/201033/6025/The-new-era-of-vulnerability-disclosure-a-brief-chat-with-HD-Moore) [HD Moore](http://en.wikipedia.org/wiki/HD_Moore)
  27. [**^**](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_ref-27) [Blog post about DLL hijacking vulnerability disclosure](http://blog.rapid7.com/?p=5325)
  28. [**^**](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29#cite_ref-28) [OWASP vulnerability categorization](http://www.owasp.org/index.php/Category:Vulnerability)

**External links**

* Security advisories links from the Open Directory <http://www.dmoz.org/Computers/Security/Advisories_and_Patches/>