

Projects

Publications

Topics

News & Updates

Events

Glossary

About CSRC

GLOSSARY

A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P
Q
R
S
T
U
V
W
X
Y
Z

vulnerability



Definitions:

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Sources:

[FIPS 200](#) under VULNERABILITY from CNSSI 4009 - Adapted
[NIST SP 1800-15B](#) under Vulnerability from [NIST SP 800-37 Rev. 2](#)
[NIST SP 1800-15C](#) under Vulnerability from [NIST SP 800-37 Rev. 2](#)
[NIST SP 1800-25B](#) under Vulnerability from [FIPS 200](#), [CNSSI 4009-2015](#) - Adapted
[NIST SP 1800-26B](#) under Vulnerability from [FIPS 200](#), [CNSSI 4009-2015](#) - Adapted
[NIST SP 1800-27B](#) under Vulnerability from [FIPS 200](#)
[NIST SP 800-124r2](#) from [NIST SP 800-53 Rev. 5](#)
[NIST SP 800-128](#) under Vulnerability from CNSSI 4009 - Adapted
[NIST SP 800-137](#) under Vulnerability from CNSSI 4009
[NIST SP 800-161r1-upd1](#) [11/1/2024 errata update] from [NIST SP 800-53 Rev. 5](#)
[NIST SP 800-18 Rev. 1](#) under Vulnerability from CNSSI 4009 - Adapted
[NIST SP 800-53 Rev. 5](#) from [NIST SP 800-30 Rev. 1](#)
[NIST SP 800-53A Rev. 5](#) from [NIST SP 800-30 Rev. 1](#)
[NIST SP 800-60 Vol. 1 Rev. 1](#) under Vulnerability from CNSSI 4009 - Adapted
[NIST SP 800-60 Vol. 2 Rev. 1](#) under Vulnerability from CNSSI 4009 - Adapted
[NISTIR 7621 Rev. 1](#) under Vulnerability
[NISTIR 7622](#) under Vulnerability from [FIPS 200](#), [NIST SP 800-115](#)

Weakness in a system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat.

Sources:

[NIST SP 1800-17b](#) under Vulnerability

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Sources:

[CNSSI 4009-2015](#) from [NIST SP 800-30 Rev. 1](#)
[NIST SP 1800-21B](#) under Vulnerability from [NIST SP 800-30 Rev. 1](#)
[NIST SP 800-12 Rev. 1](#) under Vulnerability from [NIST SP 800-30 Rev. 1](#)
[NIST SP 800-30 Rev. 1](#) under Vulnerability from CNSSI 4009
[NIST SP 800-39](#) under Vulnerability from CNSSI 4009
[NIST SP 800-82r3](#) from [FIPS 200](#)
[NISTIR 8011 Vol. 4](#) from [CNSSI 4009-2015](#)

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Note: The term weakness is synonymous for deficiency. Weakness may result in security and/or privacy risks.

Sources:

[NIST SP 800-128](#) from [CNSSI 4009-2015](#) - Adapted
[NIST SP 800-37 Rev. 2](#) from [CNSSI 4009-2015](#)

GLOSSARY COMMENTS

Comments about specific definitions should be sent to the authors of the linked Source publication. For NIST publications, an email is usually found within the document.

Comments about the glossary's presentation and functionality should be sent to secglossary@nist.gov.

See [NISTIR 7298 Rev. 3](#) for additional details.

Orca Security Ltd.
Exhibit 2176
Wiz v. Orca
IPR2024-01109

Ex. 2176-001

controls, or implementation that could be exploited or triggered by a threat source.
Note: The term weakness is synonymous for deficiency. Weakness may result in security and/or privacy risks.

Sources:

[NIST SP 800-128](#) from [CNSSI 4009-2015](#) - Adapted

[NIST SP 800-37 Rev. 2](#) from [CNSSI 4009-2015](#)

Weakness in an information system, or in system security procedures, internal controls, or implementation, that could be exploited or triggered by a threat source.

Sources:

[NIST SP 800-115](#) under Vulnerability

A flaw or weakness in a computer system, its security procedures, internal controls, or design and implementation, which could be exploited to violate the system security policy.

Sources:

[NIST SP 800-28 Version 2](#) under Vulnerability

A security exposure in an operating system or other system software or application software component. A variety of organizations maintain publicly accessible databases of vulnerabilities based on the version numbers of software. Each vulnerability can potentially compromise the system or network if exploited.

Sources:

[NIST SP 800-44 Version 2](#) under Vulnerability

[NIST SP 800-45 Version 2](#) under Vulnerability

A weakness in a system, application, or network that is subject to exploitation or misuse.

Sources:

[NIST SP 800-61 Rev. 2](#) under Vulnerability

A weakness that can be exploited or triggered to produce an adverse effect.

Sources:

[NIST SP 800-160v1r1](#)

The inability to withstand adversity.

Sources:

[NIST SP 800-160v1r1](#)

A condition that enables a threat event to occur.

Sources:

[NIST SP 800-221](#)

A weakness in system security procedures, system design, implementation, internal controls, etc., that could be exploited to violate the system security policy.

Sources:

[NISTIR 4734](#) under Vulnerability

a bug, flaw, weakness, or exposure of an application, system, device, or service that could lead to a failure of confidentiality, integrity, or availability

Sources:

[NISTIR 7435](#) under Vulnerability

An error, flaw, or mistake in computer software that permits or causes an unintended behavior to occur. CVE is a common means of enumerating vulnerabilities.

Sources:

[NISTIR 7511 Rev. 4](#) under Vulnerability

A weakness in system security procedures, hardware, design, implementation, internal controls, technical controls, physical controls, or other controls that could be accidentally triggered or intentionally exploited and result in a violation of the system's security policy.

 A weakness that can be exploited or triggered to produce an adverse effect.

Sources:

[NIST SP 800-160v1r1](#)

 The inability to withstand adversity.

Sources:

[NIST SP 800-160v1r1](#)

 A condition that enables a threat event to occur.

Sources:

[NIST SP 800-221](#)

 A weakness in system security procedures, system design, implementation, internal controls, etc., that could be exploited to violate the system security policy.

Sources:

[NISTIR 4734](#) under Vulnerability

 a bug, flaw, weakness, or exposure of an application, system, device, or service that could lead to a failure of confidentiality, integrity, or availability

Sources:

[NISTIR 7435](#) under Vulnerability

 An error, flaw, or mistake in computer software that permits or causes an unintended behavior to occur. CVE is a common means of enumerating vulnerabilities.

Sources:

[NISTIR 7511 Rev. 4](#) under Vulnerability

 A weakness in system security procedures, hardware, design, implementation, internal controls, technical controls, physical controls, or other controls that could be accidentally triggered or intentionally exploited and result in a violation of the system's security policy.

Sources:

[NISTIR 7316](#) under Vulnerability

 A condition that enables a threat event to occur.

Sources:

[NISTIR 8286](#) under Vulnerability

 A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Sources:

[NIST IR 8270](#)

[NIST IR 8323r1](#) from [NIST SP 800-30 Rev. 1](#)

[NIST IR 8401](#) from [NIST SP 800-30 Rev. 1](#) - adapted

[NIST IR 8441](#) from [NIST SP 800-30 Rev. 1](#)



HEADQUARTERS
100 Bureau Drive
Gaithersburg, MD 20899

[Contact Us](#) | [Our Other Offices](#)



Want updates about CSRC and our publications? [Subscribe](#)

Send inquiries to csrc-inquiry@nist.gov

[Site Privacy](#) | [Accessibility](#) | [Privacy Program](#) | [Copyrights](#) | [Vulnerability Disclosure](#) | [No Fear Act Policy](#) | [FOIA](#) | [Environmental Policy](#) |

[Scientific Integrity](#) | [Information Quality Standards](#) | [Commerce.gov](#) | [Science.gov](#) | [USA.gov](#) | [Vote.gov](#)