

- General +
- Vulnerabilities +
- Vulnerability Metrics +
- Products +
- Developers +
- Contact NVD
- Other Sites +
- Search +



Understanding Vulnerability Detail Pages



Vulnerability Statuses

Vulnerabilities

All vulnerabilities in the NVD have been assigned a CVE identifier and thus, abide by the definition below.

CVE defines a vulnerability as:

"A weakness in the computational logic (e.g., code) found in software and hardware components that, when exploited, results in a negative impact to confidentiality, integrity, or availability. Mitigation of the vulnerabilities in this context typically involves coding changes, but could also include specification changes or even specification deprecations (e.g., removal of affected protocols or functionality in their entirety)."

The Common Vulnerabilities and Exposures (CVE) Program's primary purpose is to uniquely identify vulnerabilities and to associate specific versions of code bases (e.g., software and shared libraries) to those vulnerabilities. The use of CVEs ensures that two or more parties can confidently refer to a CVE identifier (ID) when discussing or sharing information about a unique vulnerability. For detailed information regarding CVE please refer to <https://cve.org/> or the CNA Rules at <https://www.cve.org/ResourcesSupport/AllResources/CNARules>.

Created September 20, 2022 , Updated August 3, 2023

- General** +
- Vulnerabilities** +
- Vulnerability Metrics** +
- Products** +
- Developers** +
- Contact NVD**
- Other Sites** +
- Search** +



Understanding Vulnerability Detail Pages



Vulnerability Statuses

Vulnerabilities

All vulnerabilities in the NVD have been assigned a CVE identifier and thus, abide by the definition below.

CVE defines a vulnerability as:

"A weakness in the computational logic (e.g., code) found in software and hardware components that, when exploited, results in a negative impact to confidentiality, integrity, or availability. Mitigation of the vulnerabilities in this context typically involves coding changes, but could also include specification changes or even specification deprecations (e.g., removal of affected protocols or functionality in their entirety)."

The Common Vulnerabilities and Exposures (CVE) Program's primary purpose is to uniquely identify vulnerabilities and to associate specific versions of code bases (e.g., software and shared libraries) to those vulnerabilities. The use of CVEs ensures that two or more parties can confidently refer to a CVE identifier (ID) when discussing or sharing information about a unique vulnerability. For detailed information regarding CVE please refer to <https://cve.org/> or the CNA Rules at <https://www.cve.org/ResourcesSupport/AllResources/CNARules>.

Created September 20, 2022, Updated August 3, 2023



HEADQUARTERS
100 Bureau Drive
Gaithersburg, MD 20899
(301) 975-2000

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



**Incident Response Assistance and Non-NVD Related
Technical Cyber Security Questions:**
US-CERT Security Operations Center
Email: soc@us-cert.gov
Phone: 1-888-282-0870

[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](#)