



# CVE-2005-4900

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |                                                                                                                             |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2005-4900                                                                                                               |
| <b>State</b>           | PUBLIC                                                                                                                      |
| <b>Assigner</b>        | cve@mitre.org                                                                                                               |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                |
| <b>Published</b>       | 2016-10-14 16:59:00 UTC                                                                                                     |
| <b>Updated</b>         | 2020-12-09 09:15:00 UTC                                                                                                     |
| <b>Description</b>     | SHA-1 is not collision resistant, which makes it easier for context-dependent attackers to conduct spoofing attacks, as dem |

## Risk And Classification

### Problem Types: CWE-326

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                 | Product                | Version | Update | Edition | Language |
|-------------|------------------------|------------------------|---------|--------|---------|----------|
| Application | <a href="#">Google</a> | <a href="#">Chrome</a> | All     | All    | All     | All      |

## References

| Reference                                                                                                                               |
|-----------------------------------------------------------------------------------------------------------------------------------------|
| McAfee Security Bulletin - Database Security update fixes one vulnerability (CVE-2020-7339)                                             |
| Google Online Security Blog: Announcing the first SHA1 collision                                                                        |
| At death's door for years, widely used SHA1 function is now dead   Ars Technica                                                         |
| SHA-0/SHA-1 Reduced Operation Digest Collision Weakness                                                                                 |
| SHAttered                                                                                                                               |
| SHA-1 Broken - Schneier on Security                                                                                                     |
| Cryptology ePrint Archive: Report 2007/474                                                                                              |
| The Shappening                                                                                                                          |
| Google Online Security Blog: An update on SHA-1 certificates in Chrome                                                                  |
| CWI and Google announce first collision for Industry Security Standard SHA-1   CWI Amsterdam   Research in mathematics and computer sci |
| Schneier on Security: New Cryptanalytic Results Against SHA-1                                                                           |
| CVE Program record                                                                                                                      |
| NVD vulnerability detail                                                                                                                |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)