



CVE-1999-0007

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

Summary

| | |
|------------------------|--|
| CVE | CVE-1999-0007 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 1998-06-26 04:00:00 UTC |
| Updated | 2020-04-02 13:31:00 UTC |
| Description | Information from SSL-encrypted sessions via PKCS #1. |

Risk And Classification

Problem Types: CWE-327

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|---------------------------|--|---------|--------|---------|----------|
| Application | C2net | Stonghold Web Server | 2.0.1 | All | All | All |
| Application | C2net | Stonghold Web Server | 2.2 | All | All | All |
| Application | C2net | Stonghold Web Server | 2.3 | All | All | All |
| Application | C2net | Stonghold Web Server | 2.0.1 | All | All | All |
| Application | C2net | Stonghold Web Server | 2.2 | All | All | All |
| Application | C2net | Stonghold Web Server | 2.3 | All | All | All |
| Application | Hp | Open Market Secure Webserver | 2.1 | All | All | All |
| Application | Hp | Open Market Secure Webserver | 2.1 | All | All | All |
| Application | Microsoft | Exchange Server | 5.5 | - | All | All |
| Application | Microsoft | Exchange Server | 5.5 | - | All | All |
| Application | Microsoft | Internet Information Server | 3.0 | All | All | All |
| Application | Microsoft | Internet Information Server | 4.0 | All | All | All |
| Application | Microsoft | Internet Information Server | 3.0 | All | All | All |
| Application | Microsoft | Internet Information Server | 4.0 | All | All | All |
| Application | Microsoft | Site Server | 3.0 | All | All | All |
| Application | Microsoft | Site Server | 3.0 | All | All | All |
| Application | Netscape | Certificate Server | 1.0 | patch1 | All | All |

| | | | | | | |
|-------------|----------|--------------------|--------|--------|-----|-----|
| Application | Netscape | Certificate Server | 1.0 | patch1 | All | All |
| Application | Netscape | Collabra Server | 3.5.2 | All | All | All |
| Application | Netscape | Collabra Server | 3.5.2 | All | All | All |
| Application | Netscape | Directory Server | 1.3 | patch5 | All | All |
| Application | Netscape | Directory Server | 3.1 | patch1 | All | All |
| Application | Netscape | Directory Server | 3.12 | All | All | All |
| Application | Netscape | Directory Server | 1.3 | patch5 | All | All |
| Application | Netscape | Directory Server | 3.1 | patch1 | All | All |
| Application | Netscape | Directory Server | 3.12 | All | All | All |
| Application | Netscape | Enterprise Server | 2.0 | All | All | All |
| Application | Netscape | Enterprise Server | 3.0.1b | All | All | All |
| Application | Netscape | Enterprise Server | 3.5.1 | All | All | All |
| Application | Netscape | Enterprise Server | 2.0 | All | All | All |
| Application | Netscape | Enterprise Server | 3.0.1b | All | All | All |
| Application | Netscape | Enterprise Server | 3.5.1 | All | All | All |
| Application | Netscape | Fasttrack Server | 3.01b | All | All | All |
| Application | Netscape | Fasttrack Server | 3.01b | All | All | All |
| Application | Netscape | Messaging Server | 3.54 | All | All | All |
| Application | Netscape | Messaging Server | 3.54 | All | All | All |
| Application | Netscape | Proxy Server | 3.5.1 | All | All | All |
| Application | Netscape | Proxy Server | 3.5.1 | All | All | All |
| Application | Ssleay | Ssleay | 0.6.6 | All | All | All |
| Application | Ssleay | Ssleay | 0.8.1 | All | All | All |
| Application | Ssleay | Ssleay | 0.9 | All | All | All |
| Application | Ssleay | Ssleay | 0.6.6 | All | All | All |
| Application | Ssleay | Ssleay | 0.8.1 | All | All | All |
| Application | Ssleay | Ssleay | 0.9 | All | All | All |

References

| Reference | Source | Link | Tags |
|--|---------|---|------------------------|
| Microsoft Security Bulletin MS98-002 - Critical Microsoft Docs | MS | docs.microsoft.com | Patch, Vendor Advisory |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

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](#).

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