



CVE-1999-1085

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

Summary

CVE	CVE-1999-1085
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	1998-06-12 04:00:00 UTC
Updated	2016-10-18 02:01:00 UTC
Description	SSH 1.2.25, 1.2.23, and other versions, when used in in CBC (Cipher Block Chaining) or CFB (Cipher Feedback 64 bits) m

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ssh	Secure Shell	1.2.23	All	All	All
Application	Ssh	Secure Shell	1.2.25	All	All	All
Application	Ssh	Secure Shell	1.2.23	All	All	All
Application	Ssh	Secure Shell	1.2.25	All	All	All

References

Reference	Source	Link	Tags
'CORE-SDI-04: SSH insertion attack' - MARC	BUGTRAQ	marc.info	
ISS X-Force Database: ssh-insert (1126): SSH can accept inserted data in encrypted sessions	XF	www.iss.net	
CERT/CC Vulnerability Note VU#13877	CERT-VN	www.kb.cert.org	US Governr
'UPDATE: SSH insertion attack' - MARC	BUGTRAQ	marc.info	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

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](#)