



CVE-2015-8313

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

Summary

CVE	CVE-2015-8313
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-12-20 14:15:00 UTC
Updated	2020-01-09 17:47:00 UTC
Description	GnuTLS incorrectly validates the first byte of padding in CBC modes

Risk And Classification

Problem Types: CWE-203

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Gnu	Gnutls	All	All	All	All

References

Reference	Source	Link
1287572 – (CVE-2015-8313) CVE-2015-8313 gnutls: First byte of the padding in CBC mode is not checked	MISC	bugzilla.redhat.com
GnuTLS Padding Oracle Information Disclosure Vulnerability	MISC	www.securityfocus
SecurityFocus	MISC	www.securityfocus
CVE-2015-8313	MISC	security-tracker.de
Debian -- Security Information -- DSA-3408-1 gnutls26	MISC	www.debian.org
A little POODLE left in GnuTLS (old versions) - Hanno's blog	MISC	blog.hannoblog.de

A little POODLE left in gnutls (old versions) - Hanno's blog	MISC	blog.h00p3r.de
Bug 957568 – VUL-0: CVE-2015-8313: gnutls: First byte of the padding in CBC mode is not checked	MISC	bugzilla.suse.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report