



CVE-2019-5010

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

Summary

CVE	CVE-2019-5010
State	PUBLIC
Assigner	talos-cna@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-10-31 21:15:00 UTC
Updated	2023-11-07 03:11:00 UTC
Description	An exploitable denial-of-service vulnerability exists in the X509 certificate parser of Python.org Python 2.7.11 / 3.6.6. A spec

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Application	Python	Python	All	All	All	All
Application	Python	Python	All	All	All	All
Application	Python	Python	All	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.1	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	8.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.6	All	All	All

References

Reference	Source	Link	Tags
TALOS-2019-0758 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	MISC	talosintelligence.com	Exploit, Third
[SECURITY] [DLA 2280-1] python3.5 security update	MLIST	lists.debian.org	
Red Hat Customer Portal	REDHAT	access.redhat.com	
Pony Mail!		lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	
Python: Multiple vulnerabilities (GLSA 202003-26) — Gentoo security	GENTOO	security.gentoo.org	
[security-announce] openSUSE-SU-2020:0086-1: important: Security update	SUSE	lists.opensuse.org	
Red Hat Customer Portal	REDHAT	access.redhat.com	
[SECURITY] [DLA 2337-1] python2.7 security update	MLIST	lists.debian.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[296081](#) Oracle Solaris 11.4 Support Repository Update (SRU) 12.5.0 Missing (CPUJUL2019)

[377306](#) Alibaba Cloud Linux Security Update for python (ALINUX2-SA-2019:0094)

[377387](#) Alibaba Cloud Linux Security Update for python3 (ALINUX3-SA-2021:0080)

[500583](#) Alpine Linux Security Update for python2

[500589](#) Alpine Linux Security Update for python3

[501370](#) Alpine Linux Security Update for python3-tkinter

[504339](#) Alpine Linux Security Update for python3

[750463](#) OpenSUSE Security Update for python3 (openSUSE-SU-2020:2333-1)

[750464](#) OpenSUSE Security Update for python3 (openSUSE-SU-2020:2332-1)

© 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