



CVE-2020-26137

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2020-26137
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-30 18:15:00 UTC
Updated	2023-10-08 14:15:00 UTC
Description	urllib3 before 1.25.9 allows CRLF injection if the attacker controls the HTTP request method, as demonstrated by inserting

Risk And Classification

Problem Types: CWE-74

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edi
Operating System	Canonical	Ubuntu Linux	16.04	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All
Operating System	Canonical	Ubuntu Linux	20.04	All	All
Operating System	Debian	Debian Linux	9.0	All	All
Application	Oracle	Communications Cloud Native Core Network Function Cloud Native Environment	22.2.0	All	All
Application	Oracle	Zfs Storage Appliance Kit	8.8	All	All
Application	Python	Urllib3	All	All	All
Application	Python	Urllib3	All	All	All

References

Reference	Source	Link
[SECURITY] [DLA 2686-1] python-urllib3 security update	MLIST	lists.debian
[SECURITY] [DLA 3610-1] python-urllib3 security update	MLIST	lists.debian
Raise ValueError if method contains control characters by sethmlarson · Pull Request #1800 · urllib3/urllib3 · GitHub	MISC	github.com
Oracle Critical Patch Update Advisory - October 2021	MISC	www.oracle
USN-4570-1: urllib3 vulnerability Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu
Issue 39603: [security] http.client: HTTP Header Injection in the HTTP method - Python tracker	MISC	bugs.python

Raise ValueError if method contains control characters (#1800) · urllib3/urllib3@1dd69c5 · GitHub	MISC	github.com
Oracle Critical Patch Update Advisory - July 2022	N/A	www.oracle.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.

Legacy QID Mappings

159199 Oracle Enterprise Linux Security Update for python-urllib3 (ELSA-2021-1631)
159342 Oracle Enterprise Linux Security Update for python27:2.7 (ELSA-2021-1761)
159958 Oracle Enterprise Linux Security Update for python (ELSA-2022-5235)
178673 Debian Security Update for python-urllib3 (DLA 2686-1)
239307 Red Hat Update for python27:2.7 (RHSA-2021:1761)
239324 Red Hat Update for python-urllib3 (RHSA-2021:1631)
240523 Red Hat Update for python (RHSA-2022:5235)
257179 CentOS Security Update for python (CESA-2022:5235)
296070 Oracle Solaris 11.4 Support Repository Update (SRU) 28.82.3 Missing (CPUOCT2020)
352386 Amazon Linux Security Advisory for python-urllib3: ALAS2-2021-1668
377245 Alibaba Cloud Linux Security Update for python (ALINUX2-SA-2022:0032)
377557 Alibaba Cloud Linux Security Update for python27:2.7 (ALINUX3-SA-2022:0112)
501478 Alpine Linux Security Update for py3-urllib3
504334 Alpine Linux Security Update for py3-urllib3
6000046 Debian Security Update for python-urllib3 (DLA 3610-1)
670727 EulerOS Security Update for python-urllib3 (EulerOS-SA-2021-2485)
670783 EulerOS Security Update for python-urllib3 (EulerOS-SA-2021-2541)
670807 EulerOS Security Update for python-urllib3 (EulerOS-SA-2021-2565)
670870 EulerOS Security Update for python-urllib3 (EulerOS-SA-2021-2485)
750482 OpenSUSE Security Update for python-urllib3 (openSUSE-SU-2020:2282-1)
750493 OpenSUSE Security Update for python-urllib3 (openSUSE-SU-2020:2237-1)
750994 SUSE Enterprise Linux Security Update for aws-cli, python-boto3, python-botocore, python-service_identity, python-trustme,

python-urllib3 (SUSE-SU-2021:2817-1)
750999 OpenSUSE Security Update for aws-cli, python-boto3, python-botocore, python-service_identity, python-trustme, python-urllib3 (openSUSE-SU-2021:2817-1)
751069 OpenSUSE Security Update for aws-cli, python-boto3, python-botocore, python-service_identity, python-trustme, python-urllib3 (openSUSE-SU-2021:1206-1)
751183 SUSE Enterprise Linux Security Update for python-urllib3 (SUSE-SU-2021:3251-1)
770046 Red Hat OpenShift Container Platform 4.5.27 Packages and Security Update (RHSA-2021:0034)
770108 Red Hat OpenShift Container Platform 4.5 Security Update (RHSA-2021-0034)
900194 CBL-Mariner Linux Security Update for python-urllib3 1.24.2
903598 Common Base Linux Mariner (CBL-Mariner) Security Update for python-urllib3 (3694)
940235 AlmaLinux Security Update for python-urllib3 (ALSA-2021:1631)
940311 AlmaLinux Security Update for python27:2.7 (ALSA-2021:1761)
960310 Rocky Linux Security Update for python-urllib3 (RLSA-2021:1631)
960420 Rocky Linux Security Update for python27:2.7 (RLSA-2021:1761)
980324 Python (pip) Security Update for urllib3 (GHSA-wqvq-5m8c-6g24)

© [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](#)