



CVE-2020-11078

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

Summary

CVE	CVE-2020-11078
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-05-20 16:15:00 UTC
Updated	2023-11-07 03:14:00 UTC
Description	In httpLib2 before version 0.18.0, an attacker controlling unescaped part of uri for `httpLib2.Http.request()` could change requ

Risk And Classification

Problem Types: CWE-93

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Application	HttpLib2 Project	HttpLib2	All	All	All	All
Application	HttpLib2 Project	HttpLib2	All	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 31 Update: python-httpLib2-0.18.1-3.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
Pony Mail!		lists.apache.org
[SECURITY] Fedora 32 Update: python-httpLib2-0.18.1-3.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] [DLA 2232-1] python-httpLib2 security update	MLIST	lists.debian.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!	MLIST	lists.apache.org

[SECURITY] Fedora 31 Update: python-httplib2-0.18.1-3.fc31 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.or
Pony Mail!	MLIST	lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!		lists.apache.org
CWE-93 CRLF injection in httpplib2 · Advisory · httpplib2/httpplib2 · GitHub	CONFIRM	github.com
Pony Mail!	MLIST	lists.apache.org
Pony Mail!		lists.apache.org
Pony Mail!	MLIST	lists.apache.org
IMPORTANT security vulnerability CWE-93 CRLF injection · httpplib2/httpplib2@a1457cc · GitHub	MISC	github.com
Pony Mail!		lists.apache.org
[SECURITY] Fedora 32 Update: python-httplib2-0.18.1-3.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.or
Pony Mail!		lists.apache.org
Pony Mail!		lists.apache.org
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

[159680](#) Oracle Enterprise Linux Security Update for resource-agents security and bug fix update (ELSA-2020-5004)

[356229](#) Amazon Linux Security Advisory for python-httpplib2 : ALASANSIBLE2-2023-007

[356481](#) Amazon Linux Security Advisory for python-httpplib2 : ALAS2ANSIBLE2-2023-007

[377530](#) Alibaba Cloud Linux Security Update for fence-agents (ALINUX2-SA-2020:0178)

[378148](#) Virtuozzo Linux Security Update for fence-agents-mpath (VZLSA-2020:5003)

[378215](#) Virtuozzo Linux Security Update for resource-agents-aliyun (VZLSA-2020:5004)

[750016](#) SUSE Enterprise Linux Security Update for python-httpplib2 (SUSE-SU-2021:1637-1)

[750086](#) SUSE Enterprise Linux Security Update for python-httpplib2 (SUSE-SU-2021:1806-1)

[750087](#) SUSE Enterprise Linux Security Update for python-httpplib2 (SUSE-SU-2021:1807-1)

[750195](#) OpenSUSE Security Update for python-httpplib2 (openSUSE-SU-2021:0772-1)

[750764](#) OpenSUSE Security Update for python-httpplib2 (openSUSE-SU-2021:1806-1)

[983131](#) Python (pip) Security Update for httpplib2 (GHSA-gg84-qgv9-w4pq)

© [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](#).

Free CVE JSON API [cve.report/api](#)

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