



CVE-2023-32681

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

Summary

CVE	CVE-2023-32681
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-05-26 18:15:00 UTC
Updated	2023-09-17 09:15:00 UTC
Description	Requests is a HTTP library. Since Requests 2.3.0, Requests has been leaking Proxy-Authorization headers to destination s

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	37	All	All	All
Application	Python	Requests	All	All	All	All

References

Reference	Source	Link
Merge pull request from GHSA-j8r2-6x86-q33q · psf/requests@74ea7cf · GitHub	MISC	github.com
[SECURITY] Fedora 37 Update: python-requests-2.28.1-3.fc37 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproject.org
Release v2.31.0 · psf/requests · GitHub	MISC	github.com
[SECURITY] [DLA 3456-1] requests security update	MISC	lists.debian.org
Unintended leak of Proxy-Authorization header · Advisory · psf/requests · GitHub	MISC	github.com
[SECURITY] Fedora 38 Update: mingw-python-requests-2.31.0-1.fc38 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproject.org
Requests: Information Leak (GLSA 202309-08) — Gentoo security	MISC	security.gentoo.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

[160831](#) Oracle Enterprise Linux Security Update for python-requests (ELSA-2023-4350)

[160861](#) Oracle Enterprise Linux Security Update for python-requests (ELSA-2023-4520)

[161146](#) Oracle Enterprise Linux Security Update for python39:3.9 and python39-devel:3.9 (ELSA-2023-7034)

[161154](#) Oracle Enterprise Linux Security Update for python27:2.7 (ELSA-2023-7042)

[161165](#) Oracle Enterprise Linux Security Update for python38:3.8 and python38-devel:3.8 (ELSA-2023-7050)

[181876](#) Debian Security Update for requests (DLA 3456-1)

[199408](#) Ubuntu Security Notification for Requests Vulnerability (USN-6155-1)

[199579](#) Ubuntu Security Notification for Requests Vulnerability (USN-6155-2)

[241889](#) Red Hat Update for python-requests (RHSA-2023:4350)

[241928](#) Red Hat Update for python-requests (RHSA-2023:4520)

[242344](#) Red Hat Update for rh-python38-python (RHSA-2023:6793)

[242347](#) Red Hat Update for Satellite 6.14 (RHSA-2023:6818)

[242414](#) Red Hat Update for python39:3.9 and python39-devel:3.9 (RHSA-2023:7034)

[242431](#) Red Hat Update for python38:3.8 and python38-devel:3.8 (RHSA-2023:7050)

[242436](#) Red Hat Update for python27:2.7 (RHSA-2023:7042)

[242722](#) Red Hat Update for python-requests (RHSA-2024:0299)

[283999](#) Fedora Security Update for python (FEDORA-2023-078e257f1c)

[284096](#) Fedora Security Update for mingw (FEDORA-2023-f3824383be)

[284106](#) Fedora Security Update for python (FEDORA-2023-521ebb9cbb)

[355605](#) Amazon Linux Security Advisory for python3-requests : ALAS2-2023-2111

[355612](#) Amazon Linux Security Advisory for python-requests : ALAS2-2023-2110

[355638](#) Amazon Linux Security Advisory for python-requests : ALAS2023-2023-236

[673269](#) EulerOS Security Update for python-pip (EulerOS-SA-2023-2626)

[673284](#) EulerOS Security Update for python-pip (EulerOS-SA-2023-2596)

[673286](#) EulerOS Security Update for python-requests (EulerOS-SA-2023-2597)

[673305](#) EulerOS Security Update for python-requests (EulerOS-SA-2023-2627)

[673358](#) EulerOS Security Update for python-requests (EulerOS-SA-2023-2665)

[673414](#) EulerOS Security Update for python-requests (EulerOS-SA-2023-2822)

673428 EulerOS Security Update for python-pip (EulerOS-SA-2023-2821)
673541 EulerOS Security Update for python-pip (EulerOS-SA-2023-3151)
673625 EulerOS Security Update for python-requests (EulerOS-SA-2023-2707)
673813 EulerOS Security Update for python-pip (EulerOS-SA-2023-2797)
673854 EulerOS Security Update for python-requests (EulerOS-SA-2023-3152)
673967 EulerOS Security Update for python-requests (EulerOS-SA-2023-2798)
710749 Gentoo Linux Requests Information Leak Vulnerability (GLSA 202309-08)
754188 SUSE Enterprise Linux Security Update for python-requests (SUSE-SU-2023:2866-1)
754189 SUSE Enterprise Linux Security Update for python-requests (SUSE-SU-2023:2865-1)
754230 SUSE Enterprise Linux Security Update for python-requests (SUSE-SU-2023:3094-1)
755886 SUSE Enterprise Linux Security Update for python-requests (SUSE-SU-2023:2638-1)
755887 SUSE Enterprise Linux Security Update for python3-requests (SUSE-SU-2023:2883-1)
907016 Common Base Linux Mariner (CBL-Mariner) Security Update for python-requests (26963-1)
907030 Common Base Linux Mariner (CBL-Mariner) Security Update for python-requests (26985-1)
941199 AlmaLinux Security Update for python-requests (ALSA-2023:4350)
941219 AlmaLinux Security Update for python-requests (ALSA-2023:4520)
941465 AlmaLinux Security Update for python38:3.8 and python38-devel:3.8 (ALSA-2023:7050)
941467 AlmaLinux Security Update for python39:3.9 and python39-devel:3.9 (ALSA-2023:7034)
941480 AlmaLinux Security Update for python27:2.7 (ALSA-2023:7042)
961065 Rocky Linux Security Update for Satellite (RLSA-2023:6818)

© [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](#)