



# CVE-2021-29921

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2021-29921
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-05-06 13:15:00 UTC
<b>Updated</b>	2023-05-03 11:15:00 UTC
<b>Description</b>	In Python before 3,9,5, the ipaddress library mishandles leading zero characters in the octets of an IP address string. This (

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Oracle	Communications Cloud Native Core Automated Test Suite	1.8.0	All	All	All
Application	Oracle	Communications Cloud Native Core Binding Support Function	1.11.0	All	All	All
Application	Oracle	Communications Cloud Native Core Network Slice Selection Function	1.8.0	All	All	All
Application	Oracle	Graalvm	20.3.2	All	All	All
Application	Oracle	Graalvm	21.1.0	All	All	All
Application	Oracle	Zfs Storage Appliance Kit	8.8	All	All	All
Application	Python	Python	All	All	All	All
Application	Python	Python	All	All	All	All
Application	Python	Python	All	All	All	All

## References

### Reference

bpo-36384: Leading zeros in IPv4 addresses are no longer tolerated by tiran · Pull Request #25099 · python/cpython · GitHub

ipaddress leading zeros in IPv4 address — Python Security 0.0 documentation

Oracle Critical Patch Update Advisory - April 2022

cpython/3.8.0a4.rst at 63298930fb531ba2bb4f23bc3b915dbf1e17e9e1 · python/cpython · GitHub

Oracle Critical Patch Update Advisory - July 2021

Issue 36384: [security] CVE-2021-29921: ipaddress Should not reject IPv4 addresses with leading zeroes as ambiguously octal - Python track

[Oracle Critical Patch Update Advisory - October 2021](#)

[Oracle Critical Patch Update Advisory - January 2022](#)

[security/SICK-2021-014.md at master · sickcodes/security · GitHub](#)

[Python, PyPy3: Multiple Vulnerabilities \(GLSA 202305-02\) — Gentoo security](#)

[CVE-2021-29921 Python Vulnerability in NetApp Products | NetApp Product Security](#)

[sickcodes \(sickcodes\) · GitHub](#)

[CVE-2021-29921 - python stdlib "ipaddress" - Improper Input Validation of octal literals in python 3.8.0 thru v3.10 results in indeterminate SSP](#)

[bpo-36384: Remove check for leading zeroes in IPv4 addresses by TV4Fun · Pull Request #12577 · python/cpython · GitHub](#)

[ipaddress — IPv4/IPv6 manipulation library — Python 3.9.4 documentation](#)

[Oracle Critical Patch Update Advisory - July 2022](#)

[CVE Program record](#)

[NVD vulnerability detail](#)



No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[159466](#) Oracle Enterprise Linux Security Update for python39:3.9 and python39-devel:3.9 (ELSA-2021-4160)

[159467](#) Oracle Enterprise Linux Security Update for python38:3.8 and python38-devel:3.8 (ELSA-2021-4162)

[198392](#) Ubuntu Security Notification for Python vulnerability (USN-4973-1)

[198529](#) Ubuntu Security Notification for Python Vulnerability (USN-4973-2)

[239580](#) Red Hat Update for rh-python38 (RHSA-2021:3254)

[239841](#) Red Hat Update for python39:3.9 and python39-devel:3.9 (RHSA-2021:4160)

[239845](#) Red Hat Update for python38:3.8 and python38-devel:3.8 (RHSA-2021:4162)

[296068](#) Oracle Solaris 11.4 Support Repository Update (SRU) 34.94.4 Missing (CPUAPR2021)

[356244](#) Amazon Linux Security Advisory for python38 : ALASPYTHON3.8-2023-009

[375538](#) Python3 RFI/SSRF Vulnerability

[502021](#) Alpine Linux Security Update for python3

[504347](#) Alpine Linux Security Update for python3

[672336](#) EulerOS Security Update for python-pip (EulerOS-SA-2022-2740)

[672356](#) EulerOS Security Update for python-pip (EulerOS-SA-2022-2775)

[672442](#) EulerOS Security Update for python-pip (EulerOS-SA-2022-2854)

<a href="#">672444</a> EulerOS Security Update for python-pip (EulerOS-SA-2022-2828)
<a href="#">710714</a> Gentoo Linux Python, PyPy3 Multiple Vulnerabilities (GLSA 202305-02)
<a href="#">751095</a> OpenSUSE Security Update for python39 (openSUSE-SU-2021:2940-1)
<a href="#">940526</a> AlmaLinux Security Update for python38:3.8 and python38-devel:3.8 (ALSA-2021:4162)
<a href="#">940559</a> AlmaLinux Security Update for python39:3.9 and python39-devel:3.9 (ALSA-2021:4160)
<a href="#">960239</a> Rocky Linux Security Update for python39:3.9 and python39-devel:3.9 (RLSA-2021:4160)
<a href="#">960342</a> Rocky Linux Security Update for python38:3.8 and python38-devel:3.8 (RLSA-2021:4162)

© [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](#)**